COMUNE DI CANEGRATE PROVINCIA DI MILANO CODICE 10934	NUMERO 165	DATA 25-11-2020

OGGETTO:
APPROVAZIONE PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

COPIA

DELIBERAZIONE DELLA GIUNTA COMUNALE

SI DÀ ATTO CHE, AI SENSI DELL'ART. 73 DL 17/03/2020 N. 18 E SUCCESSIVI, E DEL DECRETO SINDACALE N. 5 DEL 23/03/2020, LA SEDUTA DI GIUNTA COMUNALE SI È TENUTA IN MODALITÀ VIDEOCONFERENZA TRAMITE PIATTAFORMA GOTOMEETING, IL GIORNO **25/11/2020** ALLE ORE **18.00.**

ALL'APPELLO RISULTANO:

COMPONENTE	P.	A.G.	A.I.	COMPONENTE	P.	A.G.	A.I.
COLOMBO ROBERTO	X			MERAVIGLIA FRANCA	X		
MODICA MATTEO	X			SPIRITO DAVIDE	X		
AUTERI GIUSEPPINA	X			ZAMBON EDOARDO	X		

TOTALE PRESENTI 6 TOTALE ASSENTI 0

ASSISTE IL SEGRETARIO GENERALE DOTT.SSA TERESA LA SCALA

ESSENDO LEGALE IL NUMERO DEGLI INTERVENUTI, IL SINDACO ROBERTO COLOMBO ASSUME LA PRESIDENZA E DICHIARA APERTA LA SEDUTA, PER LA TRATTAZIONE DELL'OGGETTO SOPRA INDICATO.

COMUNE DI CANEGRATE (MILANO)

DELIBERAZIONE DI GIUNTA COMUNALE N. 165 DEL 25/11/2020

OGGETTO: APPROVAZIONE PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

LA GIUNTA COMUNALE

Premesso:

che la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale é un diritto fondamentale e che l'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano;

che il Parlamento Europeo e il Consiglio dell'Unione Europea hanno approvato il 27 aprile 2016 il Regolamento generale per la protezione dei dati personali (UE) 2016/679 (in seguito solo Regolamento o GDPR), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, abrogando la Direttiva 95/46/CE ;

rilevato che il GDPR è diventato definitivamente applicabile in via diretta in ciascuno degli Stati membri dell'Unione Europea a partire dal 25 maggio 2018;

richiamato il D. Lgs. 30/06/2003, n. 196 c.d. *Codice della privacy*, considerato il referente normativo principale della materia, profondamente modificato con il D. Lgs. 10/08/2018 n. 101, con il quale si è armonizzata la normativa interna con quella sovranazionale, in attuazione della delega contenuta nell'art. 13 Legge 25 ottobre 2017 n. 166 (legge di delegazione europea 2016/2017).

Rilevato che, con il GDPR, è stato richiesto agli Stati membri:

- un quadro più solido e coerente in materia di protezione dei dati, affiancato da efficaci misure di adeguamento, data l'importanza di creare il clima di fiducia funzionale allo sviluppo dell'economia digitale in tutto il mercato interno;

Ritenuto che l'adeguamento dell'ordinamento nazionale interno al GDPR renda necessario definire le politiche e gli obiettivi strategici da conseguire per garantire l'adeguamento;

Ritenuto che l'obiettivo di assicurare la sicurezza dei dati richiede di gestire efficacemente, e conformemente alle disposizioni del GDPR, il rischio di violazione dei dati derivante dal trattamento, per tale dovendosi intendere 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 e che, a tal fine, vadano definiti gli obiettivi correlati alla gestione del rischio;

Ritenuto, pertanto, necessario procedere alla approvazione di un piano di protezione dei dati personali e di gestione del rischio di violazione.

Visto l'allegato schema di Piano;

Appurato che:

- lo schema di piano copre il periodo del triennio 2020-2022
- la funzione principale dello stesso è quella di assicurare il processo, a ciclo continuo, di adozione, modificazione, aggiornamento e adeguamento del processo di gestione del rischio e della strategia di sicurezza, secondo i principi, le disposizioni e le linee guida elaborate a livello nazionale e internazionale;
- il documento consente che la strategia si sviluppi e si modifichi in modo da mettere via via a punto degli strumenti di protezione mirati e sempre più incisivi;
- l'adozione del documento non si configura come un'attività una tantum, bensì come un processo continuo in cui le strategie e gli strumenti vengono via via affinati, modificati o sostituiti in relazione al feedback ottenuto dalla loro applicazione;
- eventuali aggiornamenti successivi, anche infra annuali, correlati agli esiti dei monitoraggi o alla sopravvenienza di nuove normative o prassi ovvero alla necessità di conformarsi a provvedimenti e/o pareri dell'autorità di controllo o del RPD, sono oggetto di approvazione da parte dello stesso organo che ha approvato il PPD.

Considerato che lo schema di Piano è stato predisposto dal responsabile del procedimento con il coinvolgimento e la partecipazione degli attori indicati nello Schema di Piano medesimo e, in particolare con la partecipazione dei dirigenti/responsabili P.O. e il coinvolgimento del responsabile dei sistemi informativi;

Rilevato che il Responsabile del procedimento è il Responsabile dell'Area Affari Generali.

Dato atto che il Responsabile del procedimento, al fine di garantire il livello essenziale delle prestazioni, è tenuto a garantire la pubblicazione del presente provvedimento e dello schema di piano allegato sul sito web dell'Amministrazione, nella apposita sezione "Amministrazione trasparente" e nella sottosezione "Altri contenuti-anticorruzione".

Visti:

- il D. Lgs. 267/2000;
- il Regolamento UE n. 679/2016;
- le linee guida adottate dal Gruppo di Lavoro art. 29 sulla protezione dei dati;
- le indicazioni fornite dall'Autorità Garante per la Protezione dei Dati personali e dal Responsabile Protezione Dati del Comune di Canegrate.

Acquisito il parere di regolarità tecnica, reso ai sensi dell'art. 49 comma 1 del TUEL, dal Responsabile del Servizio interessato.

con voti unanimi favorevoli resi nella forma di legge;

DELIBERA

per le ragioni indicate in narrativa, e che qui si intendono integralmente richiamate:

1. di approvare il Piano di Protezione dei Dati Personali e Gestione del Rischio di Violazione, allegato al presente atto per farne parte integrante e sostanziale;

2. Di dare atto che il Piano copre il periodo di un triennio, 2020-2022 ed è soggetto ad aggiornamento annuale, e ad aggiornamenti anche infrannuali correlati agli esiti dei monitoraggi o alla sopravvenienza di nuove normative o prassi ovvero alla necessità di conformarsi a provvedimenti e/o pareri dell'autorità di controllo o del RPD;

3. Di comunicare i contenuti del Piano a tutti i soggetti indicati nel Piano medesimo, attraverso i canali dallo stesso individuati, e di demandare ai dirigenti/responsabili P.O. nonché a tutti i dipendenti l'attuazione del Piano.

Con successiva votazione unanime la presente è dichiarata immediatamente eseguibile ai sensi dell'art. 134 comma 4, del D. Lgs. 267/2000.

Si allega:
- Piano di Protezione dei Dati Personali e Gestione del Rischio di Violazione
- Parere preventivo reso ai sensi dell'art. 49 comma 1 del TUEL

COMUNE DI CANEGRATE

Città Metropolitana di Milano

AREA AFFARI GENERALI

Parere preventivo art. 49 e art. 147 bis comma 1 Decreto Legislativo 18 agosto 2000, n. 267

Allegato alla deliberazione n. 165 assunta in data 25 NOV. 2020

☒ GIUNTA COMUNALE ☐ CONSIGLIO COMUNALE

OGGETTO: **APPROVAZIONE PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE**

In relazione al presente atto si esprime parere favorevole di regolarità tecnica.

Canegrate,

IL RESPONSABILE AREA AFFARI GENERALI
(D.ssa Teresa La Scala)

COMUNE DI CANEGRATE (MILANO)

COMUNE DI CANEGRATE (MILANO)

Comune di CANEGRATE
(Città Metropolitana di Milano)
Sede: via A. Manzoni, 1 - Tel. (0331) 463811 - Telefax (0331) 401535 - Cod. fisc. e part. IVA 00835500158
www.comune.canegrate.mi.it

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE[1]

per una gestione del rischio robusta

approvato in adeguamento della norma UNI ISO 31000
e conforme al REGOLAMENTO UE 2016/679

[1] Il paragrafo 5.5.3 della norma UNI ISO 31000 prevede la predisposizione e l'adeguamento di "PIANI DI TRATTAMENTO DEL RISCHIO" aventi lo scopo di documentare come le opzioni di trattamento scelte sono attuate e indica, altresi', le informazioni da fornire nei suddetti piani.

RIFERIMENTI DOCUMENTALI

Titolo del Documento	Piano di protezione dei dati
Numero di versione	01
Data ultimo aggiornamento	07/10/2020
Stato del documento	Approvato dal Titolare con proprio provvedimento
Estensori del documento	Comune di Canegrate (MI)
Riferimento per comunicazioni in merito al documento	Tel. 0331 463814 segreteria@comune.canegrate.mi.it
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	Pubblicazione sul sito web istituzionale nella sezione Amministrazione Trasparente

Titolo del Documento: Piano di protezione dei dati
Numero di versione: 01

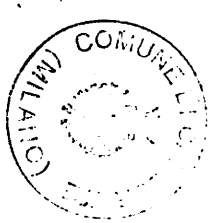
Data ultimo aggiornamento 07/10/2020

Stato del documento: Approvato dal Titolare con proprio provvedimento

Estensori del documento: Comune di Canegrate (MI)

Riferimento per comunicazioni in merito al documento: Tel. 0331 463814

Modalita' di distribuzione del presente documento e delle eventuali nuove versioni: Pubblicazione sul sito web istituzionale nella sezione Amministrazione Trasparente



PARTE I
PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE (PPD)

DEFINIZIONI
Il presente documento recepisce e utilizza le seguenti definizioni:
- GDPR: 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, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (GDPR generale sulla protezione dei dati);

- 'WP29': gruppo di lavoro articolo 29 sulla protezione dei dati, per tale dovendosi intendere il Gruppo di lavoro istituito in virtu' dell'articolo 29 della direttiva 95/46/CE quale organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata con i suoi compiti fissati all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE;

- 'PPD': il presente Piano di Protezione dei Dati personali e gestione del rischio di violazione;

- 'Regolamento dati sensibili': il Regolamento interno, approvato dal titolare in conformita' allo schema tipo approvato dal Garante, che identifica e rende pubblici, per i trattamenti dei dati sensibili e giudiziari, i tipi di dati e le operazioni eseguibili;

- 'ID': identificativo.

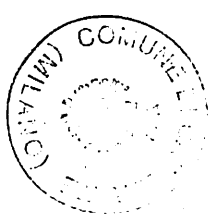
Recepisce e utilizza, altresi', le seguenti definizioni:

A) ai fini del D.Lgs. n. 196/2003:

- 'trattamento': qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

- 'dato personale': qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

- 'dati identificativi': i dati personali che permettono l'identificazione diretta dell'interessato;



elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un contraente o utente ricevente, identificato o identificabile;

- 'chiamata': la connessione istituita da un servizio di comunicazione elettronica accessibile al pubblico che consente la comunicazione bidirezionale;

- 'reti di comunicazione elettronica': i sistemi di trasmissione e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse, inclusi gli elementi di rete non attivi, che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

- 'rete pubblica di comunicazioni': una rete di comunicazione elettronica utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico, che supporta il trasferimento di informazioni tra i punti terminali di reti;

- 'servizio di comunicazione elettronica': i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002;

- 'contraente': qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate;

- 'utente': qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;

- 'dati relativi al traffico': qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;

- 'dati relativi all'ubicazione': ogni dato trattato in una rete di comunicazione elettronica o da un servizio di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;

- 'servizio a valore aggiunto': il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto e' necessario per la trasmissione di una comunicazione o della relativa fatturazione;

- 'posta elettronica': messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza;

- 'dato personale': qualsiasi informazione riguardante una persona fisica identificata o identificabile ('interessato'); si considera identificabile la persona fisica che puo' 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 piu' elementi caratteristici della sua identita' 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 del trattamento': il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

- 'profilazione': qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilita', il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

- 'pseudonimizzazione': il trattamento dei dati personali in modo tale che i dati personali non possano piu' essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

- 'archivio': qualsiasi insieme di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

- 'titolare del trattamento': la persona fisica o giuridica, l'autorita' pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalita' e i mezzi del trattamento di dati personali; quando le finalita' 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'autorita' pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

- 'destinatario': la persona fisica o giuridica, l'autorita' pubblica, il servizio o altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorita' 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 autorita' pubbliche e' conforme alle norme applicabili in materia di protezione dei dati secondo le finalita' del trattamento;

responsabile del trattamento in uno o piu' paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attivita' economica comune;

- 'autorita' di controllo': l'autorita' pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR;

- 'autorita' di controllo interessata': un'autorita' di controllo interessata dal trattamento di dati personali in quanto:

a) il titolare del trattamento o il responsabile del trattamento e' stabilito sul territorio dello Stato membro di tale autorita' di controllo;

b) gli interessati che risiedono nello Stato membro dell'autorita' di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento;

oppure

c) un reclamo e' stato proposto a tale autorita' di controllo;

- 'trattamento transfrontaliero':

a) trattamento di dati personali che ha luogo nell'ambito delle attivita' di stabilimenti in piu' di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in piu' di uno Stato membro;

oppure

b) trattamento di dati personali che ha luogo nell'ambito delle attivita' di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in piu' di uno Stato membro;

- 'obiezione pertinente e motivata': un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al predente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle liberta' fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

- 'servizio della societa' dell'informazione': il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio;

- 'organizzazione internazionale': un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o piu' Stati.

Per quanto concerne i trattamenti senza l'ausilio di strumenti elettronici, secondo il D.Lgs. n. 196/2003, tale trattamento e' consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative;

b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;

c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalita' di accesso finalizzata all'identificazione degli incaricati.

FINALITA'

Il presente documento, in attuazione del GDPR e della normativa interna di adeguamento, e' funzionale alla protezione dei diritti e delle liberta' fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali trattati nell'esercizio dell'attivita' istituzionale in un quadro di garanzie per gli interessati che contempla nuovi diritti. Sul presupposto che costituisce un OBIETTIVO STRATEGICO la sicurezza del trattamento dei dati personali, scopo del presente documento e' programmare e pianificare gli interventi affinche' i dati personali siano:
a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ('liceita', correttezza e trasparenza');

b) raccolti per finalita' determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalita'; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non e', conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalita' iniziali ('limitazione della finalita");

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalita' per le quali sono trattati ('minimizzazione dei dati');

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalita' per le quali sono trattati ('esattezza');

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'adeguamento di misure tecniche e organizzative adeguate richieste dal presente GDPR a tutela dei diritti e delle liberta' dell'interessato ('limitazione della conservazione');

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali ('integrita' e riservatezza').

- Parere del WP29 sulla limitazione della finalita' - 13/EN WP 203;

- Norme internazionali;

- Regolamenti interni, approvati dai titolari e/o dai responsabili.

CORRELAZIONE CON IL PTPC E GLI ALTRI STRUMENTI DI PIANIFICAZIONE

La violazione dei dati personali, intesa come 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, e' rilevante ai fini del PTPC e degli altri strumenti di programmazione dell'Ente.
La correlazione tra i diversi strumenti di programmazione viene garantita sia in fase di elaborazione sia in fase di adeguamento.

DATA E PROVVEDIMENTO DI APPROVAZIONE

L'organo competente dell'intestato titolare ha approvato il PPD con provvedimento nr..... Xxx..... del..... xxxx.

PERIODO DI RIFERIMENTO E MODALITA' DI AGGIORNAMENTO

Il PPD copre il periodo del triennio 2020-2022, e la funzione principale dello stesso e' quella di assicurare il processo, a ciclo continuo, di adozione, modificazione, aggiornamento e adeguamento del processo di gestione del rischio e della strategia di sicurezza, secondo i principi, le disposizioni e le linee guida elaborate a livello nazionale e internazionale.
Il documento consente che la strategia si sviluppi e si modifichi in modo da mettere via via a punto degli strumenti di protezione mirati e sempre piu' incisivi.

In questa logica, l'adozione del documento non si configura come un'attivita' una tantum, bensi' come un processo continuo in cui le strategie e gli strumenti vengono via via affinati, modificati o sostituiti in relazione al feedback ottenuto dalla loro applicazione.

Eventuali aggiornamenti successivi, anche infra annuali, correlati agli esiti dei monitoraggi o alla sopravvenienza di nuove normative o prassi, sono oggetto di approvazione da parte dello stesso organo che ha approvato il PPD.

ATTORI INTERNI ALL'AMMINISTRAZIONE CHE HANNO PARTECIPATO ALLA PREDISPOSIZIONE DEL PIANO, NONCHE' CANALI E STRUMENTI DI PARTECIPAZIONE

Oltre al titolare, hanno contribuito alla predisposizione del Piano, per quanto di propria competenza:
- contitolari;.

PARTE II
DATI PERSONALI, RISCHIO DI VIOLAZIONE E DISCIPLINA DEL GDPR

IL RISCHIO PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E LA NEUTRALIZZAZIONE DEL RISCHIO ATTRAVERSO IL SISTEMA DI PROTEZIONE BASATO SU UNI ISO 31000

Nell'attuale contesto, lo sviluppo e la rapidita' dell'evoluzione tecnologica nonche' la globalizzazione comportano nuove sfide per la protezione dei dati personali. Sempre piu' spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. Nel contempo, la tecnologia attuale consente a soggetti pubblici e privati di utilizzare dati personali come mai in precedenza, e la portata della condivisione e della raccolta di dati personali e' aumentata in modo significativo. Tale evoluzione richiede un quadro piu' solido e coerente in materia di protezione dei dati, tenuto conto dell'aumento del rischio di violazione dei dati medesimi e della necessita' che le persone fisiche abbiano il controllo dei dati personali che li riguardano in un quadro di certezza giuridica e operativa rafforzata cosi' come delineata del GDPR.

Il rischio inerente al trattamento e' da intendersi come rischio di impatti negativi sulle liberta' e sui diritti degli interessati.

Rispetto a tali possibili impatti negativi, il titolare del trattamento e' tenuto a promuovere e adottare approcci e politiche che tengano conto costantemente del rischio, effettuando una analisi attraverso un apposito processo di valutazione (si vedano artt. 35-36 GDPR) che sappia tenere conto:

- dei rischi noti o evidenziabili;

- delle misure tecniche e organizzative adottate o che si intende adottare per mitigare il rischio.

A tale fine, il titolare del trattamento, attraverso il sistema di protezione, promuove e adotta approcci e politiche che tengano conto costantemente del rischio, introducendo:

- l'obbligo di effettuare valutazioni di impatto (DPIA) prima di procedere ad un trattamento di dati che presenti rischi elevati per i diritti delle persone, e di consultare l'Autorita' di protezione dei dati in caso di dubbi;

- adeguate misure di sicurezza;

- un sistema di monitoraggio sull'efficacia delle misure;

- la figura del "Responsabile della protezione dei dati" (RPD/DPO).

Il delineato sistema di protezione vale per:

- la quantita' dei dati personali raccolti;

- la portata del trattamento;

- il periodo di conservazione;

- l'accessibilita'.

Resta fermo che l'adesione a un meccanismo di certificazione, approvato ai sensi dell'articolo 42 GDPR, puo' essere utilizzato come elemento per dimostrare la conformita' ai requisiti.

L'ACCOUNTABILITY QUALE CONSEGUENZA DELL'APPROCCIO BASATO SUL RISCHIO

Accountability: Registro e ricognizione dei trattamenti

Il sistema di protezione "by default and by design" si fonda sull'assunto che il titolare del trattamento o un suo delegato:
- e' competente per il pieno e rigoroso rispetto del sistema di protezione dei dati personali e, in particolare, per il rispetto dei principi di "liceita', correttezza e trasparenza", "limitazione della finalita'", "minimizzazione dei dati", "esattezza", "limitazione della conservazione" e "integrita' e riservatezza";

- e' in grado di comprovare il rispetto del sistema di protezione e dei relativi principi in base al principio di "responsabilizzazione" (accountability).

In tale modo viene affidato al titolare il compito di:

- decidere autonomamente le modalita', le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel GDPR.

Sulla base di tale impostazione, il GDPR pone con forza l'accento sulla "responsabilizzazione" (accountability) del titolare e dei responsabili, ossia sull'adozione di:

- comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del GDPR.

Accountability: Registro e ricognizione dei trattamenti

Il principio di responsabilizzazione richiede che il titolare e i responsabili di trattamento istituiscano e tengano costantemente aggiornato, in forma scritta, anche elettronica:

Sulla base di tale elenco, non esaustivo ma meramente esemplificativo, la valutazione in ordine alla concreta identificazione e adeguamento delle misure e' rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da art. 32 del GDPR, fermo restando che l'adesione a specifici codici di condotta o a schemi di certificazione puo' essere utilmente effettuata per attestare l'adeguatezza delle misure di sicurezza adottate. Per tale motivo, dopo il 25 maggio 2018, vengono meno obblighi generalizzati di adozione di misure "minime" di sicurezza (ex art. 33 D.Lgs. n. 196/2003). In ogni caso, la sicurezza del trattamento attraverso l'adozione e attuazione di adeguate misure richiede altresi' che il titolare del trattamento e il responsabile del trattamento facciano si' che chiunque agisca sotto la loro autorita' e abbia accesso a dati personali non tratti tali dati se non e' istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Cio' premesso, ai fini della concreta individuazione delle misure di sicurezza, anche riferimento alle prescrizioni gia' contenute, in particolare, nell'Allegato "B" al D.Lgs. n. 196/2003, il titolare e i responsabili del trattamento tengono in considerazione anche:

- le linee guida o buone prassi indicate dal Garante sulla base dei risultati positivi conseguiti negli anni;

- le misure di sicurezza previste per i trattamenti di dati sensibili svolti dai soggetti pubblici per finalita' di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi ai sensi degli artt. 20 e 22 D.Lgs. n. 196/2003 e del Regolamento sui dati sensibili adottato dall'Ente conformemente allo Schema tipo di GDPR per il trattamento dei dati sensibili e giudiziari dei comuni, del 19 settembre 2005.

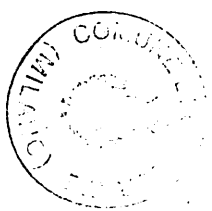
Accountability: Notifica delle violazioni di dati personali
Il principio di responsabilizzazione impone che, in caso di violazione dei dati personali:

- il titolare del trattamento notifichi la violazione all'autorita' di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne e' venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le liberta' delle persone fisiche e impone altresi' che, qualora la notifica all'autorita' di controllo non sia effettuata entro 72 ore, la stessa venga corredata dei motivi del ritardo;

- il titolare del trattamento documenti qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio posto che tale documentazione consente all'autorita' di controllo di verificare il rispetto della disciplina in tema di notifiche di violazioni;

- il responsabile del trattamento informi il titolare del trattamento, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione;

- il titolare del trattamento comunichi la violazione all'interessato senza ingiustificato ritardo quando la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le liberta' delle persone fisiche, salve le eccezioni previste dall'art. 34 par. 3 GDPR.



c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;

d) cooperare con l'autorita' di controllo;

e) fungere da punto di contatto per l'autorita' di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

La sua designazione e' obbligatoria e, in relazione alle caratteristiche soggettive e oggettive di indipendenza, autorevolezza, competenze manageriali, il titolare del trattamento e il responsabile del trattamento:

- si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali;

- sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica

- si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti e che il responsabile della protezione dei dati non sia rimosso o penalizzato per l'adempimento dei propri compiti;

- si assicurano che i compiti e funzioni non diano adito a un conflitto di interessi.

Il SISTEMA DI PROTEZIONE E I FONDAMENTI DI LICEITA' DEL TRATTAMENTO

Raccomandazioni Garante

L'approccio basato sul rischio e sulla responsabilizzazione sono strumentali alla realizzazione di una efficace protezione dei dati personali, le quale non puo' che fondarsi:

- sulla liceita' del trattamento e sulla relativa base giuridica.

Liceita' del trattamento.

I fondamenti di liceita' e la base giuridica del trattamento sono indicati all'art. 6 del GDPR:

-consenso

- adempimento obblighi contrattuali;

- interessi vitali della persona interessata o di terzi;

In definitiva:

- per i dati "sensibili" il consenso deve essere "esplicito"; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati, compresa la profilazione;

- non deve essere necessariamente "documentato per iscritto", ne' e' richiesta la "forma scritta", anche se questa e' modalita' idonea a configurare l'inequivocabilita' del consenso e il suo essere "esplicito" (per i dati sensibili) e a dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento;

- il consenso dei minori e' valido a partire dai 16 anni fermo restando che il limite di eta' puo' essere abbassato fino a 13 anni dalla normativa nazionale; prima di tale eta' occorre raccogliere il consenso dei genitori o di chi ne fa le veci;

- deve essere, in tutti i casi, libero, specifico, informato e inequivocabile e non e' ammesso il consenso tacito o presunto (no a caselle prespuntate su un modulo)

- deve essere manifestato attraverso "dichiarazione o azione positiva inequivocabile".

Cio' premesso, il consenso raccolto precedentemente al 25 maggio 2018 resta valido se ha tutte le caratteristiche sopra individuate. In caso contrario, e' opportuno adoperarsi prima di tale data per raccogliere nuovamente il consenso degli interessati secondo quanto prescrive il GDPR, se si vuole continuare a fare ricorso a tale base giuridica.

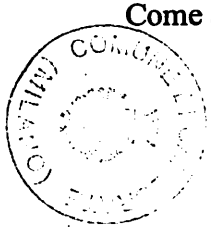
In particolare, occorre verificare che la richiesta di consenso sia:

- chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato (art. 7.2), per esempio all'interno di modulistica.

Occorre prestare attenzione alla formula utilizzata per chiedere il consenso: deve essere comprensibile, semplice, chiara, fermo restando che i soggetti pubblici non devono, di regola, chiedere il consenso per il trattamento dei dati personali.

Relativamente alla lett. b) e all'interesse vitale di un terzo, si puo' invocare tale base giuridica solo se nessuna delle altre condizioni di liceita' puo' trovare applicazione. Il GDPR offre alcuni criteri per il bilanciamento in questione e soprattutto appare utile fare riferimento al documento pubblicato dal Gruppo "Articolo 29" sul punto "Base giuridica".

Come anzi evidenziato, il trattamento dei dati richiede la presenza di una base giuridica su cui fondarsi.



e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

Raccomandazioni del Garante

Il presente PPD tiene conto e recepisce le raccomandazioni del Garante secondo cui i titolari dovrebbero condurre la propria valutazione alla luce di questi principi sotto indicati:

- il regolamento offre alcuni criteri per il bilanciamento fra legittimo interesse del titolare o del terzo e diritti e liberta' dell'interessato (si veda considerando 47) e soprattutto appare utile fare riferimento al documento pubblicato dal Gruppo "Articolo 29" sul punto (WP217);

- si confermano, inoltre, nella sostanza, i requisiti indicati dall'Autorita' nei propri provvedimenti in materia di bilanciamento di interessi con particolare riferimento agli esiti delle verifiche preliminari condotte dall'Autorita', con eccezione ovviamente delle disposizioni che il regolamento ha espressamente abrogato (per esempio: obbligo di notifica dei trattamenti).

Il SISTEMA DI PROTEZIONE E L'INFORMATIVA

Contenuti dell'informativa

I contenuti dell'informativa sono elencati in modo tassativo negli articoli 13, paragrafo 1, e 14, paragrafo 1, del GDPR.
In particolare, il titolare DEVE SEMPRE specificare:

- i dati di contatto del RPD-DPO ove esistente;

- la base giuridica del trattamento;

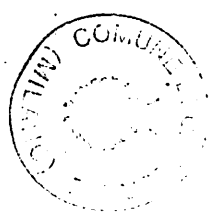
- il suo interesse legittimo se quest'ultimo costituisce la base giuridica del trattamento;

- se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti.

Il GDPR prevede anche ulteriori informazioni in quanto "necessarie per garantire un trattamento corretto e trasparente": in particolare, il titolare deve specificare:

- il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione;

- il diritto di presentare un reclamo all'autorita' di controllo.



- quali sono i destinatari dei dati.

Ogni volta che le finalita' cambiano e' necessario informarne l'interessato prima di procedere al trattamento ulteriore.

Raccomandazioni del Garante sull'informativa

Il presente PPD tiene conto e recepisce le raccomandazioni del Garante, di seguito indicate:

- prima del 25 maggio 2018, verificare la rispondenza delle informative utilizzate a tutti i criteri delineati dal GDPR, con particolare riguardo ai contenuti obbligatori e alle modalita' di redazione, in modo da apportare le modifiche o le integrazioni eventualmente necessarie prima di tale scadenza;

- fermo restando che il GDPR supporta chiaramente il concetto di informativa "stratificata", piu' volte esplicitato dal Garante nei suoi provvedimenti in particolare attraverso l'impiego di icone associate (in vario modo) a contenuti piu' estesi, che devono essere facilmente accessibili, e promuove l'utilizzo di strumenti elettronici per garantire la massima diffusione e semplificare la prestazione delle informative, una volta adeguata l'informativa nei termini sopra indicati, i titolari potranno continuare o iniziare a utilizzare queste modalita' per la prestazione dell'informativa, comprese le icone che l'Autorita' ha in questi anni suggerito nei suoi provvedimenti (videosorveglianza, banche, ecc.) - in attesa della definizione di icone standardizzate da parte della Commissione;

- vanno adottate anche le misure organizzative interne idonee a garantire il rispetto della tempistica:

- il termine di 1 mese per l'informativa all'interessato e' chiaramente un termine massimo, e occorre ricordare che l'art. 14, paragrafo 3, lettera a), del GDPR menziona in primo luogo che il termine deve essere "ragionevole";

- poiche' spetta al titolare valutare lo sforzo sproporzionato richiesto dall'informare una pluralita' di interessati, qualora i dati non siano stati raccolti presso questi ultimi, e salva l'esistenza di specifiche disposizioni normative nei termini di cui all'art. 23, paragrafo 1, del GDPR, e' utile fare riferimento ai criteri evidenziati nei provvedimenti con cui il Garante ha riconosciuto negli anni l'esistenza di tale sproporzione.

Il SISTEMA DI PROTEZIONE E I DIRITTI DEGLI INTERESSATI

Modalita' per l'esercizio dei diritti

Trasparenza e modalita' trasparenti per l'esercizio dei diritti dell'interessato sono alla base della disciplina del GDPR. In particolare, il titolare del trattamento deve agevolare l'esercizio dei diritti da parte dell'interessato, adottando ogni misura tecnica e organizzativa a cio' idonea. Benche' sia il solo titolare a dover dare riscontro in caso di esercizio dei diritti, il responsabile e' tenuto a collaborare con il titolare o un suo delegato ai fini dell'esercizio dei diritti degli interessati.

f) il diritto di proporre reclamo a un'autorita' di controllo;

g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;

h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4 GDPR, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonche' l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento.

Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento puo' addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

Il diritto di ottenere una copia di cui al paragrafo 3 dell'art. 15 GDPR non deve ledere i diritti e le liberta' altrui.

Diritto alla rettifica e cancellazione

Il presente PPD tiene conto della disciplina del GDPR in tema di diritto di rettifica e cancellazione ("diritto all'oblio"), e di seguito indicata.

Quanto al diritto di rettifica, l'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalita' del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Quanto al diritto cosiddetto "all'oblio", l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

a) i dati personali non sono piu' necessari rispetto alle finalita' per le quali sono stati raccolti o altrimenti trattati;

b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;

c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;

a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;

b) il trattamento e' illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;

c) benche' il titolare del trattamento non ne abbia piu' 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 e' opposto al trattamento ai sensi dell'articolo 21, paragrafo 1 del GDPR, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

Se il trattamento e' limitato a norma del paragrafo 1, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

L'interessato che ha ottenuto la limitazione del trattamento a norma del paragrafo 1 e' informato dal titolare del trattamento prima che detta limitazione sia revocata.

Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali limitazioni del trattamento salvo che cio' si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

Diritto alla portabilita'

Il presente PPD tiene conto della disciplina del GDPR in tema di diritto alla portabilita' dei dati, e di seguito indicata.

L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:

a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b);

b) il trattamento sia effettuato con mezzi automatizzati.

- Diritto di accesso

Oltre al rispetto delle prescrizioni relative alla modalita' di esercizio di questo e degli altri diritti (si veda "Modalita' per l'esercizio dei diritti"), il titolare puo' consentire agli interessati di consultare direttamente, da remoto e in modo sicuro, i propri dati personali.

- Diritto alla limitazione

Il diritto alla limitazione prevede che il dato personale sia "contrassegnato" in attesa di determinazioni ulteriori; pertanto, e' opportuno che il titolare preveda nei propri sistemi informativi (elettronici o meno) misure idonee a tale scopo.

- Diritto alla portabilita'

Il Gruppo "Articolo 29" ha pubblicato recentemente linee-guida specifiche dove sono illustrati e spiegati i requisiti e le caratteristiche del diritto alla portabilita' con particolare riguardo ai diritti di terzi interessati i cui dati siano potenzialmente compresi fra quelli "relativi all'interessato" di cui quest'ultimo chiede la portabilita'.

Vanno tenuti presente i numerosi provvedimenti con cui l'Autorita' ha indicato criteri per il bilanciamento fra i diritti e le liberta' fondamentali di terzi e quelli degli interessati esercitanti i diritti.

Poiche' la trasmissione dei dati da un titolare all'altro prevede che si utilizzino formati interoperabili, il titolare che ricadono nel campo di applicazione di questo diritto dovrebbero adottare sin da ora le misure necessarie a produrre i dati richiesti in un formato interoperabile.

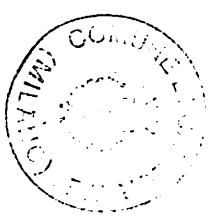
Il SISTEMA DI PROTEZIONE E I TRASFERIMENTI DI DATI VERSO PAESI TERZI E ORGANISMI INTERNAZIONALI

Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali

Il GDPR ha confermato l'approccio attualmente vigente per quanto riguarda i flussi di dati al di fuori dell'Unione europea e dello spazio economico europeo, prevedendo che tali flussi sono vietati, in linea di principio, a meno che intervengano specifiche garanzie che il regolamento elenca in ordine gerarchico:

- adeguatezza del Paese terzo riconosciuta tramite decisione della Commissione europea: il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale e' ammesso, ai sensi dell'art. 45 GDPR, se la Commissione ha deciso che il paese terzo, un territorio o uno o piu' settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche. Le decisioni di adeguatezza sinora adottate dalla Commissione (livello di protezione dati in Paesi terzi, a partire dal Privacy Shield, e clausole contrattuali tipo per titolari e responsabili) e gli accordi internazionali in materia di trasferimento dati stipulati prima del 24 maggio 2016 dagli Stati membri restano in vigore a meno di una loro eventuale revisione o modifica (si vedano art. 45,

Tuttavia, l'autorizzazione del Garante resta ancora necessaria se il titolare desidera utilizzare clausole contrattuali ad-hoc (cioe' non riconosciute come adeguate tramite decisione della Commissione europea) oppure accordi amministrativi stipulati tra autorita' pubbliche - una delle novita' introdotte dal regolamento.



norma la comunicazione e' ammessa quando e' comunque necessaria per lo svolgimento di funzioni istituzionali e puo' essere iniziata se e' decorso il termine di cui all'articolo 39, comma 2 D.Lgs. 196/2003, e non e' stata adottata la diversa determinazione ivi indicata. La comunicazione da parte di un soggetto pubblico a privati o a enti pubblici economici e la diffusione da parte di un soggetto pubblico sono ammesse unicamente quando sono previste da una norma di legge o di regolamento;

- principi applicabili al trattamento di dati sensibili: il trattamento dei dati sensibili e' consentito solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalita' di rilevante interesse pubblico perseguite. Nei casi in cui una disposizione di legge specifica la finalita' di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni eseguibili, il trattamento e' consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici acura dei soggetti che ne effettuano il trattamento, in relazione alle specifiche finalita' perseguite nei singoli casi e nel rispetto dei principi di cui all'articolo 22, D.Lgs. 196/2003, con atto di natura regolamentare adottato in conformita' al parere espresso dal Garante ai sensi dell'articolo 154, comma 1, lettera g) del decreto sopra citato, anche su schemi tipo. Se il trattamento non e' previsto espressamente da una disposizione di legge i soggetti pubblici possono richiedere al Garante l'individuazione delle attivita', tra quelle demandate ai medesimi soggetti dalla legge, che perseguono finalita' di rilevante interesse pubblico e per le quali e' conseguentemente autorizzato, ai sensi dell'articolo 26, comma 2, il trattamento dei dati sensibili. Il trattamento e' consentito solo se il soggetto pubblico provvede altresi' a identificare e rendere pubblici i tipi di dati e di operazioni nei modi di cui al comma 2. L'identificazione dei tipi di dati e di operazioni e' aggiornata e integrata periodicamente;

- principi applicabili al trattamento di dati giudiziari: il trattamento di dati giudiziari da parte di soggetti pubblici e' consentito solo se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le finalita' di rilevante interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili. Il trattamento dei dati giudiziari e' altresi' consentito quando e' effettuato in attuazione di protocolli d'intesa per la prevenzione e il contrasto dei fenomeni di criminalita' organizzata stipulati con il Ministero dell'interno o con i suoi uffici periferici di cui all'articolo 15, comma 2, del decreto legislativo 30 luglio 1999, n. 300, previo parere del Garante per la protezione dei dati personali, che specificano la tipologia dei dati trattati e delle operazioni eseguibili. Nei casi in cui una disposizione di legge specifica la finalita' di rilevante interesse pubblico, ma non i tipi di dati giudiziari e di operazioni eseguibili, il trattamento e' consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti che ne effettuano il trattamento, in relazione alle specifiche finalita' perseguite nei singoli casi e nel rispetto dei principi di cui all'articolo 22, con atto di natura regolamentare adottato in conformita' al parere espresso dal Garante ai sensi dell'articolo 154, comma 1, lettera g), anche su schemi tipo. L'identificazione dei tipi di dati e di operazioni e' aggiornata e integrata periodicamente;

- principi applicabili al trattamento di dati sensibili e giudiziari: il trattamento dei dati sensibili e giudiziari deve essere conformato secondo modalita' volte a prevenire violazioni dei diritti, delle liberta' fondamentali e della dignita' dell'interessato. Nel fornire l'informativa occorre fare espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale e' effettuato il trattamento dei dati sensibili e giudiziari. E' possibile trattare solo i dati sensibili e giudiziari indispensabili per svolgere attivita' istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa. I dati sensibili e giudiziari sono raccolti, di regola, presso l'interessato. E' necessario verificare, periodicamente, l'esattezza e l'aggiornamento dei dati sensibili e giudiziari, nonche' la loro pertinenza, completezza, non eccedenza e indispensabilita' rispetto alle finalita' perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. Al fine di

Responsabili del trattamento e sub-responsabili
Il GDPR ha modificato la definizione di responsabile del trattamento in:
- "responsabile del trattamento": la persona fisica o giuridica, l'autorita' pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Per effetto di tale modifica, il responsabile e' il soggetto esterno alla struttura organizzativa che agisce "per conto del titolare".

Il responsabile e' designato dal titolare facoltativamente. Ove necessario per esigenze organizzative, possono essere designati responsabili piu' soggetti, anche mediante suddivisione di compiti. In particolare, il titolare puo' avvalersi, per il trattamento di dati, anche sensibili, di soggetti pubblici o privati che, in qualita' di responsabili del trattamento, forniscano le garanzie del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Se designato, il responsabile e' individuato tra soggetti che per esperienza, capacita' ed affidabilita' forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando cosi' al titolare del trattamento l'opportunita' di opporsi a tali modifiche. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincola il responsabile del trattamento al titolare del trattamento e che individua la materia disciplinata e la durata del trattamento, la natura e la finalita' del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

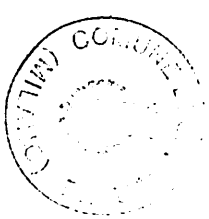
Il contratto o altro atto giuridico dettaglia, analiticamente, i compiti affidati al responsabile e prevede, in particolare, che il responsabile del trattamento:

a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui e' soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

c) adotti tutte le misure richieste ai sensi dell'articolo 32 del GDPR;

d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;



Cio' premesso in via generale in materia di responsabili del trattamento, per quanto concerne i fornitori di servizi di comunicazione elettronica accessibili al pubblico si rinvia integralmente alla disciplina degli artt. 32 e 32-bis del D.Lgs. n. 196/2003 anche per quanto concerne gli adempimenti conseguenti ad una violazione di dati personali

Incaricati
Pur non prevedendo espressamente la figura dell' "incaricato" del trattamento (ex art. 30 Codice), il GDPR non ne esclude la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorita' diretta del titolare o del responsabile".
Restano applicabili le disposizioni del D.Lgs. n. 196/20013 in tema di incaricati. In particolare:

- le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorita' del titolare o del responsabile, attenendosi alle istruzioni impartite;

- la designazione e' effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unita' per la quale e' individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unita' medesima.

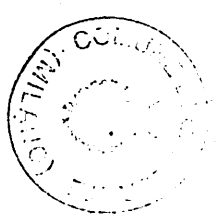
Raccomandazioni del Garante su titolare, responsabile e incaricato del trattamento
Il presente PPD tiene conto e recepisce le raccomandazioni del Garante sui fondamenti di liceita' del trattamento, di seguito indicate.
I titolari del trattamento devono valutare attentamente l'esistenza di eventuali situazioni di contitolarita', essendo obbligati in tal caso a stipulare:

- l'accordo interno di cui parla l'art. 26, paragrafo 1, del GDPR.

E' necessario, in particolare, individuare il "punto di contatto per gli interessati" previsto dal suddetto articolo ai fini dell'esercizio dei diritti previsti dal GDPR.

Il titolare di trattamento dove verificare che i contratti o altri atti giuridici che attualmente disciplinano i rapporti con i rispettivi responsabili siano conformi a quanto previsto, in particolare, dall'art. 28, paragrafo 3, del GDPR. Devono essere apportate le necessarie integrazioni o modifiche entro il 25 maggio 2018, in particolare qualora si intendano designare sub-responsabili nei termini sopra descritti.

Attraverso l'adesione a codici deontologici ovvero l'adesione a schemi di certificazione il responsabile puo' dimostrare le "garanzie sufficienti" di cui all'art. 28, paragrafi 1 e 4 del GDPR.



- sorvegliare l'osservanza del presente GDPR, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonche' delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilita', la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attivita' di controllo;

- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del DGPR;

- cooperare con l'autorita' di controllo;

- fungere da punto di contatto per l'autorita' di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Nell'eseguire i propri compiti, il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalita' del medesimo.

Il responsabile della protezione dei dati:

- va tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

- va sostenuto nell'esecuzione dei propri compiti fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica;

- non deve ricevere alcuna istruzione per quanto riguarda l'esecuzione dei propri compiti.

Il responsabile della protezione dei dati non e' rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti.

Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.

LA SICUREZZA

Misure di sicurezza

Fermo restando il principio che qualunque trattamento di dati personali da parte di soggetti pubblici e' consentito soltanto per lo svolgimento delle funzioni istituzionali e che, salvo quanto previsto dalla legge per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, i soggetti pubblici non devono richiedere il consenso dell'interessato, i trattamenti in ambito pubblico devono svolgersi in modo lecito e garantendo la sicurezza. A tal fine, il GDPR stabilisce che il titolare del trattamento attui misure adeguate per garantire ed essere in grado di dimostrare il rispetto di detto GDPR, tenendo conto tra l'altro dei "rischi aventi probabilita' e gravita' diverse per i diritti e le liberta' delle persone fisiche" (articolo 24, paragrafo 1) .

b) i legittimi interessi perseguiti dal responsabile del trattamento in contesti specifici;

c) la raccolta dei dati personali;

d) la pseudonimizzazione dei dati personali;

e) l'informazione fornita al pubblico e agli interessati;

f) l'esercizio dei diritti degli interessati;

g) l'informazione fornita e la protezione del minore e le modalita' con cui e' ottenuto il consenso del titolare della responsabilita' genitoriale sul minore;

h) le misure e le procedure di cui agli articoli 24 e 25 GDPR e le misure volte a garantire la sicurezza del trattamento di cui all'articolo 32;

i) la notifica di una violazione dei dati personali alle autorita' di controllo e la comunicazione di tali violazioni dei dati personali all'interessato;

j) il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali;

k) le procedure stragiudiziali e di altro tipo per comporre le controversie tra titolari del trattamento e interessati in materia di trattamento, fatti salvi i diritti degli interessati ai sensi degli articoli 77 e 79 GDPR.

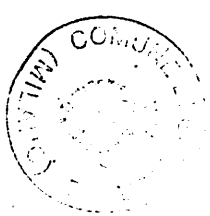
Certificazione

Gli Stati membri, le autorita' di controllo, il comitato e la Commissione incoraggiano, in particolare a livello di Unione:
- l'istituzione di meccanismi di certificazione della protezione dei dati nonche' di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformita' al presente GDPR dei trattamenti effettuati dal titolare del trattamento e dai responsabili del trattamento. Sono tenute in considerazione le esigenze specifiche delle micro, piccole e medie imprese.

La certificazione e' volontaria e accessibile tramite una procedura trasparente.

La certificazione ai sensi dell'art. 42 del GDPR non riduce la responsabilita' del titolare del trattamento o del responsabile del trattamento riguardo alla conformita' al GDPR e lascia impregiudicati i compiti e i poteri delle autorita' di controllo competenti.

La certificazione ai sensi dell'art. 42 del GDPR e' rilasciata dagli organismi di certificazione di cui all'articolo 43 del GDPR o dall'autorita' di controllo competente.



Comunicazione di una violazione dei dati personali all'interessato
Quando la violazione dei dati personali e' suscettibile di presentare un rischio elevato per i diritti e le liberta' delle persone fisiche, il titolare del trattamento:
- comunica la violazione all'interessato senza ingiustificato ritardo.

La comunicazione all'interessato descrive, con un linguaggio semplice e chiaro, la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d) del GDPR:

- comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere piu' informazioni;

- descrizione delle probabili conseguenze della violazione dei dati personali;

- descrizione delle 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.

Non e' richiesta la comunicazione all'interessato se e' soddisfatta una delle seguenti condizioni:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le liberta' degli interessati;

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorita' di controllo puo' richiedere, dopo aver valutato la probabilita' che la violazione dei dati personali presenti un rischio elevato, che vi provveda o puo' decidere che una delle condizioni sopra citate e' soddisfatta.

LA DOCUMENTAZIONE DEL SISTEMA DI PROTEZIONE
Le diverse componenti del sistema di protezione sono documentati almeno da:

PARTE IV
GESTIONE DEL RISCHIO SECONDO LA NORMA UNI ISO 31.000
Principi applicabili alla gestione del rischio
Principi applicabili alla gestione del rischio
Sulla base della Norma UNI ISO 31.000, e ai fini della strategia di protezione dei dati personali, viene definita:

- la nozione di "rischio" come uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravita' e probabilita'.

- la nozione di "gestione dei rischi" come l'insieme delle attivita' coordinate volte a indirizzare e controllare un'organizzazione in relazione ai rischi.

La gestione di rischi derivanti dal trattamento sulla protezione dei dati personali viene condotta tenendo presente i principi contenuti nella della Norma UNI ISO 31.000 e di seguito riportati.

a) La gestione del rischio crea e protegge il valore. La gestione del rischio contribuisce in maniera dimostrabile al raggiungimento degli obiettivi ed al miglioramento della prestazione, per esempio in termini di salute e sicurezza delle persone, security, rispetto dei requisiti cogenti, consenso presso l'opinione pubblica, protezione dell'ambiente, qualita' del prodotto gestione dei progetti, efficienza nelle operazioni, governance e reputazione.

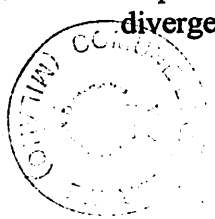
b) La gestione del rischio e' parte integrante di tutti i processi dell'organizzazione. La gestione del rischio non e' un'attivita' indipendente, separata dalle attivita' e dai processi principali dell'organizzazione. La gestione del rischio fa parte delle responsabilita' della direzione ed e' parte integrante di tutti i processi dell'organizzazione, inclusi la pianificazione strategica e tutti i processi di gestione dei progetti e del cambiamento.

c) La gestione del rischio e' parte del processo decisionale. La gestione del rischio aiuta i responsabili delle decisioni ad effettuare scelte consapevoli, determinare la scala di priorita' delle azioni e distinguere tra linee di azione alternative.

d) La gestione del rischio tratta esplicitamente l'incertezza. La gestione del rischio tiene conto esplicitamente dell'incertezza, della natura di tale incertezza e di come puo' essere affrontata.

e) La gestione del rischio e' sistematica, strutturata e tempestiva. Un approccio sistematico, tempestivo e strutturato alla gestione del rischio contribuisce all'efficienza ed a risultati coerenti, confrontabili ed affidabili.

f) La gestione del rischio si basa sulle migliori informazioni disponibili. Gli elementi in ingresso al processo per gestire il rischio si basano su fonti di informazione quali dati storici, esperienza, informazioni di ritorno dai portatori d'interesse, osservazioni, previsioni e parere di specialisti. Tuttavia, i responsabili delle decisioni dovrebbero informarsi, e tenerne conto, di qualsiasi limitazione dei dati o del modello utilizzati o delle possibilita' di divergenza di opinione tra gli specialisti.



I documenti allegati e, in particolare, la ricognizione dei trattamenti in rapporto a tutta l'attivita' dell'ente, le schede di DPIA e l'elenco dei rischi, della gravita' rilevata dalla prospettiva degli interessati e della relativa motivazione comprovano l'effettuazione della analisi dei rischi derivanti dai trattamenti, e l'accuratezza della analisi medesima.

Contesto interno organizzativo

Struttura organizzativa

La struttura organizzativa dell'Ente e' indicata nella MAPPA DELLA STRUTTURA ORGANIZZATIVA allegata, e corrisponde alle funzioni istituzionali e ai compiti assegnati a ciascuna struttura.

La **MAPPA DEI LUOGHI** indica:

- la sede principale, con l'indicazione degli Uffici e la relativa descrizione;

- le sedi secondarie, con l'indicazione degli Uffici e la relativa descrizione.

Soggetti: Titolare del trattamento

Denominazione: XXX

Sede: XXX

Punti di contatto: XXX

Il titolare del trattamento, sopra citato, esercita le funzioni e i compiti e assume le responsabilita' indicate nel GDPR e della normativa interna di recepimento.

Soggetti: Legale rappresentante del titolare del trattamento

Anagrafica: XXX

Sede: XXX

Punti di contatto: XXX

Soggetti: Contitolari del trattamento

d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;

e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui cio' sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;

f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che e' terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;

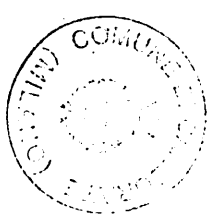
h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attivita' di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

Con riguardo alla lettera h), il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente GDPR o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attivita' di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente GDPR. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilita' dell'adempimento degli obblighi dell'altro responsabile.

L'adesione da parte del responsabile del trattamento a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 del GDPR puo' essere utilizzata come elemento per dimostrare le garanzie sufficienti.

Fatto salvo un contratto individuale tra il titolare del trattamento e il responsabile del trattamento, il contratto o altro atto giuridico di cui sopra puo' basarsi, in tutto o in parte, su clausole contrattuali tipo di cui ai paragrafi 7 e 8 dell'articolo 28 del GDPR, anche laddove siano parte di una certificazione concessa al titolare del trattamento o al responsabile del trattamento ai sensi degli articoli 42 e 43 del GDPR.



La validita' e l'efficacia del GDPR per il trattamento dei dati sensibili e giudiziari, dopo la scadenza del 25 maggio 2018, ovvero l'adeguamento del GDPR medesimo restano subordinati alle indicazioni e prescrizioni del Garante.

Schede di ricognizione dei trattamenti

Fanno parte del sistema di protezione le Schede di ricognizione dei trattamenti elaborate con riferimento a tutta l'attivita' svolta dall'Ente, prendendo in considerazione tutti i processi, inclusi i procedimenti amministrativi.

Mappa hardware

La Mappa hardware, allegata al presente documento per formarne parte integrante e sostanziale, identifica gli strumenti, i tipi di supporto e i locali di ubicazione. Fornisce, altresi', una descrizione delle caratteristiche tecniche degli strumenti elettronici medesimi.

Mappa software

La Mappa software, allegata al presente documento per formarne parte integrante e sostanziale, identifica i software in relazione agli archivi/banche dati che vengono gestiti dai software medesimi.

Identifica, altresi', i soggetti abilitati all'accesso.

Mappa dei rischi

La Mappa dei rischi, allegata al presente documento per formarne parte integrante sostanziale, costituisce un elenco dei principali eventi rischiosi che possono determinare la violazione dei dati e rileva, dalla prospettiva degli interessati, la gravita' e la correlata motivazione.

Elenco trattamenti effettuati da responsabili esterni

L'Elenco trattamenti affidati in outsourcing o effettuati da responsabili esterni, e allegato al presente documento per formarne parte integrante sostanziale, consente di rilevare il rischio derivante dai trattamenti effettuate da soggetti esterni alla struttura organizzativa dell'Ente.

Schede di determinazione preliminare della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del GDPR (UE) 2016/679

Fanno parte del sistema di protezione le Schede di determinazione preliminare della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del GDPR (UE) 2016/679, le quali vengono allegate al presente documento per formarne parte integrante sostanziale.

Si tratta di documenti:

Mappa misure di sicurezza procedurali

Fa parte integrante e sostanziale del sistema di protezione l'allegata MAPPA delle misure di sicurezza procedurali.

Elenco misure di sicurezza

Fa parte integrante e sostanziale del sistema di protezione l'allegato ELENCO misure di sicurezza, correlate alla ricognizione/indice dei trattamenti e suddivise per uffici.

Registro delle attivita' di trattamento e delle categorie di attivita'

Fanno parte integrante sostanziale del sistema di protezione:

- il Registro delle attivita' di trattamento svolte sotto la responsabilita' del titolare;

- il Registro del responsabile del trattamento contenente tutte le categorie di attivita' relative al trattamento svolte per conto del titolare.

I contenuti dei Registri devono essere conformi alle disposizioni contenute nell'articolo 30 del GDPR nonche' alle prescrizioni della normativa interna di adeguamento del GDPR e alle linee guida, raccomandazioni, indicazioni e eventuali modelli del Garante.

Altri documenti del Sistema di protezione

Costituiscono parte del sistema di protezione, per formarne parte integrante sostanziale:

- atti di delega al trattamento dei dati;

- atti di nomina degli incaricati.

Costituiscono parte del sistema di protezione, quand'anche non fisicamente allegati al presente documento, i seguenti ulteriori documenti:

- disciplinare tecnico allegato B al d.lgs. 196/2003;

- elenco misure minime ITC e relative implementazioni, adottato entro il 31 dicembre 2017;

- codice di condotta dell'Ente;

- GDPR sulla protezione dei dati laddove approvato;

PARTE V
GESTIONE DEL RISCHIO SECONDO LA NORMA UNI ISO 31.000: FASE DELLA VALUTAZIONE

Determinazione di assoggettabilita' dei trattamenti a valutazione di impatto - DPIA
In base alla Norma UNI ISO 31.000, la valutazione del rischio richiede l'identificazione, l'analisi e la ponderazione del rischio medesimo.
Ai fini della valutazione del rischio, il GDPR introduce l'obbligo di valutazione d'impatto del trattamento sulla protezione dei dati.

Una valutazione d'impatto sulla protezione dei dati e' un processo inteso a descrivere il trattamento, valutarne la necessita' e la proporzionalita', nonche' a contribuire a gestire i rischi per i diritti e le liberta' delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli.

Le valutazioni d'impatto sulla protezione dei dati sono strumenti importanti per la responsabilizzazione in quanto sostengono i titolari del trattamento non soltanto nel rispettare i requisiti del regolamento generale sulla protezione dei dati, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del GDPR.

Cio' premesso, il presente PPD tiene presente, in via generale, che:

- qualora il trattamento coinvolga contitolari del trattamento, questi ultimi devono definire con precisione le rispettive competenze. La loro valutazione d'impatto sulla protezione dei dati deve stabilire quale parte sia competente per le varie misure volte a trattare i rischi e a proteggere i diritti e le liberta' degli interessati. Ciascun titolare del trattamento deve esprimere le proprie esigenze e condividere informazioni utili senza compromettere eventuali segreti (ad esempio protezione di segreti aziendali, proprieta' intellettuale, informazioni aziendali riservate) o divulgare vulnerabilita';

- fatti salvi i casi in cui un trattamento rientra nel campo di applicazione di un'eccezione (III.B.a Linee Guida su valutazione impatto), e' necessario realizzare una valutazione d'impatto sulla protezione dei dati qualora un trattamento "possa presentare un rischio elevato", intendendosi per "rischio" uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravita' e probabilita', e per "gestione dei rischi" l'insieme delle attivita' coordinate volte a indirizzare e controllare un'organizzazione in relazione ai rischi;

- la valutazione d'impatto sulla protezione dei dati va effettuata anche per valutare l'impatto sulla protezione dei dati di un prodotto tecnologico, o, ad esempio un dispositivo hardware o un software, qualora sia probabile che lo stesso venga utilizzato da titolari del trattamento distinti per svolgere tipologie diverse di trattamento;

- la valutazione d'impatto sulla protezione dei dati puo' riguardare una singola operazione di trattamento dei dati. Tuttavia vi sono circostanze in cui puo' essere ragionevole ed economico effettuare una valutazione d'impatto sulla protezione dei dati che verta su un oggetto piu' ampio di un unico progetto. Pertanto si puo' ricorrere a una singola valutazione d'impatto sulla protezione dei dati nel caso di trattamenti multipli simili tra loro in termini di natura, ambito di applicazione, contesto, finalita' e rischi. In effetti, le valutazioni d'impatto sulla protezione dei dati mirano a studiare

- fermo restando che, secondo le Linee guida, un trattamento che soddisfa 2 criteri deve formare oggetto di una valutazione d'impatto sulla protezione dei dati, tuttavia, al fine di garantire una maggiore garanzia di tutela, la ricorrenza anche di 1 solo criterio costituisce elemento sufficiente per originare l'obbligo di svolgimento della DPIA;

- maggiore e' il numero di criteri soddisfatti dal trattamento, piu' e' probabile che sia presente un rischio elevato per i diritti e le liberta' degli interessati e, di conseguenza, che sia necessario realizzare una valutazione d'impatto sulla protezione dei dati;

- se, pur applicando i criteri sopra indicati, la necessita' di una DPIA non emerge con chiarezza, va comunque ritenuto sussistente l'obbligo - secondo quanto raccomandato dal WP29 - di farvi ricorso in quanto la DPIA contribuisce all'osservanza delle norme in materia di protezione dati da parte dei titolari di trattamento;

- la valutazione d'impatto sulla protezione dei dati non e' richiesta nei seguenti casi:

- quando, sulla base di predetti criteri, risulta che il trattamento non e' tale da "presentare un rischio elevato per i diritti e le liberta' delle persone fisiche";

- quando la natura, l'ambito di applicazione, il contesto e le finalita' del trattamento sono molto simili a un trattamento per il quale e' stata svolta una valutazione d'impatto sulla protezione dei dati. In tali casi, si possono utilizzare i risultati della valutazione d'impatto sulla protezione dei dati per un trattamento analogo;

- quando le tipologie di trattamento sono state verificate da un'autorita' di controllo prima del maggio 2018 in condizioni specifiche che non sono cambiate;

- qualora un trattamento, effettuato a norma dell'articolo 6, paragrafo 1, lettere c) o e) GPDR, trovi una base giuridica nel diritto dell'Unione o nel diritto dello Stato membro, tale diritto disciplini il trattamento specifico o sia gia' stata effettuata una valutazione d'impatto sulla protezione dei dati nel contesto dell'adozione di tale base giuridica (articolo 35, paragrafo 10 GPDR).

In ordine ai diversi trattamenti, le SCHEDE allegate per formare parte integrante e sostanziale del presente PPD, evidenziano le determinazioni assunte, tenendo conto delle linee guida adottate in materia.

Valutazione di impatto - DPIA per trattamenti a rischio elevato

In base alle determinazioni di assoggettabilita' a valutazione di impatto di cui alle allegate SCHEDE (DPIA-FASE 1), i trattamenti per i quali risulta determinato, sulla base dei CRITERI delle citate Linee guida, un elevato rischio per i diritti e le liberta' delle persone fisiche, e che non rientrano tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "GDPR") sono assoggettati a valutazione di impatto (DPIA-FASE 2).

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale;

b) il responsabile del trattamento dei dati, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie;

c) il responsabile della protezione dei dati e il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;

d) il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza.

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology (modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del GDPR:

a) una descrizione sistematica dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

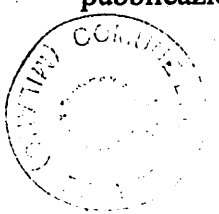
b) una valutazione della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una valutazione dei rischi per i diritti e le liberta' degli interessati di cui al paragrafo 1, art. 35 del GDPR;

d) le 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 conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Pubblicazione sintesi della valutazione d'impatto - DPIA

La pubblicazione di una valutazione d'impatto sulla protezione dei dati non e' un requisito giuridico sancito dal GDPR generale sulla protezione dei dati, e' una decisione del titolari del trattamento procedere in tal senso. Tuttavia, il titolare del trattamento dovrebbe prendere in considerazione la pubblicazione di almeno alcune parti, ad esempio di una sintesi o della conclusione della loro valutazione d'impatto sulla protezione dei dati.



Occorre tuttavia sottolineare che, indipendentemente dal fatto che la consultazione dell'autorita' di controllo sia richiesta o meno in base al livello di rischio residuo, sussistono comunque gli obblighi di conservare una registrazione della valutazione d'impatto sulla protezione dei dati e di aggiornamento di detta valutazione al momento opportuno.

Conclusioni e raccomandazioni del Garante in tema di DPIA

Le valutazioni d'impatto sulla protezione dei dati sono uno strumento utile di cui dispongono il titolare del trattamento per attuare sistemi di trattamento dei dati conformi al GDPR generale sulla protezione dei dati e possono essere obbligatorie per talune tipologie di trattamenti. Hanno natura modulabile e possono assumere forme diverse, tuttavia il GDPR generale sulla protezione dei dati stabilisce i requisiti essenziali di una valutazione d'impatto sulla protezione dei dati efficace. Il titolare del trattamento dovrebbe considerare la realizzazione di una valutazione d'impatto sulla protezione dei dati come un'attivita' utile e positiva che contribuisce alla conformita' giuridica.

L'articolo 24, paragrafo 1, definisce la responsabilita' fondamentale del titolare del trattamento in termini di rispetto del GDPR generale sulla protezione dei dati: "Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalita' del trattamento, nonche' dei rischi aventi probabilita' e gravita' diverse per i diritti e le liberta' delle persone fisiche, il titolare o un suo delegato del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento e' effettuato conformemente al presente GDPR. Dette misure sono riesaminate e aggiornate qualora necessario".

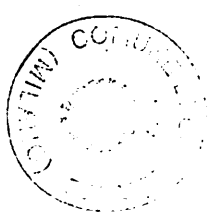
La valutazione d'impatto sulla protezione dei dati e' un aspetto fondamentale del rispetto del GDPR laddove si preveda di svolgere o si stia svolgendo un trattamento di dati soggetto a rischio elevato. Cio' significa che il titolare del trattamento dovrebbe utilizzare i criteri stabiliti nel presente documento per stabilire se devono realizzare una valutazione d'impatto sulla protezione dei dati o meno. La politica interna del titolare del trattamento potrebbe estendere questo elenco andando oltre i requisiti giuridici sanciti dal GDPR generale sulla protezione dei dati. Cio' dovrebbe suscitare un maggior senso di fiducia e riservatezza negli interessati e in altri titolari del trattamento.

Qualora si preveda di effettuare un trattamento che possa presentare un rischio elevato, il titolare del trattamento deve:

- scegliere una metodologia per la valutazione d'impatto sulla protezione dei dati (esempi riportati nell'allegato 1) che soddisfi i criteri di cui all'allegato 2, oppure specificare ed attuare un processo sistematico di valutazione d'impatto sulla protezione dei dati che:

- o sia conforme ai criteri di cui all'allegato 2;

- o sia integrata nei processi in materia di progettazione, sviluppo, cambiamento, rischio e riesame operativo in conformita' con i processi, il contesto e la cultura interni;



PARTE VI
GESTIONE DEL RISCHIO SECONDO LA NORMA UNI ISO 31.000 : FASE DEL TRATTAMENTO

Misure di sicurezza del trattamento
Il GDPR prevede che il titolare del trattamento attui misure adeguate per garantire ed essere in grado di dimostrare il rispetto di detto GDPR, tenendo conto tra l'altro dei "rischi aventi probabilita' e gravita' diverse per i diritti e le liberta' delle persone fisiche" (articolo 24, paragrafo 1). L'obbligo per il titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati va inteso nel contesto dell'obbligo generale, cui gli stessi sono soggetti, di gestire adeguatamente i rischi.

Tenendo conto dello stato dell'arte e dei costi di adeguamento, nonche' della natura, dell'oggetto, del contesto e delle finalita' del trattamento, come anche del rischio di varia probabilita' e gravita' per i diritti e le liberta' delle persone fisiche, il titolare o un suo delegato del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacita' di assicurare su base permanente la riservatezza, l'integrita', la disponibilita' e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacita' di ripristinare tempestivamente la disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 puo' essere utilizzata come elemento per dimostrare la conformita' ai requisiti di cui al paragrafo 1 del presente articolo.

Il titolare del trattamento e il responsabile del trattamento fanno si' che chiunque agisca sotto la loro autorita' e abbia accesso a dati personali non tratti tali dati se non e' istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

- Cancelli

d) Misure presenti anti incendio

- Estintori

- Idranti

- Rilevatori

d) Misure presenti per la regolarita' degli impianti

- Elettrico

- Climatizzazione

- Riscaldamento

e) Misure presenti per la continuita' elettrica

- UPS

- Generatori

f) Procedure

- Procedura di gestione degli accessi

- Procedura di gestione dei visitatori/manutentori

L'identificazione delle misure di sicurezza logistiche/fisiche prende in considerazione almeno le principali sotto indicate misure, elencate a titolo esemplificativo e non esaustivo:

a) antifurto

- Sensori

d) Sicurezza accessi

- Controllo
- Registrazione
- Altro

e) Sicurezza CED

- Adeguato posizionamento all'interno dell'edificio
- Adeguate pareti soffitto/pavimento
- Misure anti effrazione
- Controllo accessi
- Impianto di climatizzazione
- Misure antincendio idonee all'uso con le apparecchiature presenti
- Porte antincendio di adeguata dimensione
- Rilevatori di fumo, calore, allagamento

f) continuita' operativa

- Gruppo di continuita'
- Gruppo elettrogeno
- Coerenza fra i dispositivi di continuita' e le normative VVFF
- Pavimento galleggiante per l'adeguato posizionamento dei cavi.
- Corretto ed ordinato posizionamento dei cavi elettrici
- Corretto ed ordinato posizionamento dei cavi di rete

L'adeguamento dell'Ente alle Misure minime e' avvenuto entro il 31 dicembre 2017, come da documentazione in atti che si allega al presente piano per farne parte integrante e sostanziale.

Le Misure, che si articolano sull'adeguamento di controlli di natura tecnologica, organizzativa e procedurale, prevedono tre livelli di adeguamento. Il livello minimo e' quello al quale ogni pubblica amministrazione, indipendentemente dalla sua natura e dimensione, deve necessariamente essere o rendersi conforme. I livelli successivi rappresentano situazioni evolutive in grado di fornire livelli di protezione piu' completi, e dovrebbero essere adottati fin da subito dalle organizzazioni maggiormente esposte a rischi (ad esempio per la criticita' delle informazioni trattate o dei servizi erogati), ma anche visti come obiettivi di miglioramento da parte di tutte le altre organizzazioni.

Come parte del processo di adeguamento, il dirigente responsabile dell'adeguamento deve inoltre compilare e firmare digitalmente il "Modulo di implementazione" allegato alla Circolare, il quale e' reso disponibile in diversi formati editabili, da questa pagina.

AgID provvedera' ad aggiornare le Misure minime tutte le volte che si rendera' necessario, in funzione dell'evoluzione della minaccia cibernetica, al fine di mantenere la Pubblica Amministrazione ad un livello adeguato di protezione.

Fra le misure minime e' previsto anche:

- che le pubbliche amministrazioni accedano sistematicamente a servizi di early warning che consentano loro di rimanere aggiornate sulle nuove vulnerabilita' di sicurezza. A tal proposito il CERT-PA fornisce servizi proattivi ed informativi a tutte le amministrazioni accreditate.

Per l'identificazione dellee misure minime informatiche/logiche, per la sicurezza ICT ai fini del presente PPD si rinvia alle suddette misure misure minime per la sicurezza ICT delle pubbliche amministrazioni come attuate e implementate dal titolare.

La MAPPA delle misure di sicurezza logistiche/fisiche applicate i diversi trattamenti inclusi i criteri e modalita' di salvataggio e di ripristino della disponibilita' dei dati, allegata al presente PPD per formane parte integrante e sostanziale, documenta e comprova l'osservanza del GDPR.

Misure di sicurezza organizzative
A titolo esemplificativo e non esaustivo, si elencano:

- disciplinare tecnico: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al d.lgs. 196/2003 per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare a:

a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati

b) alle istruzioni da impartire agli incaricati medesimi

c) al controllo, alla custodia e restituzione della documentazione

Misure di sicurezza procedurali
Le misure di sicurezza organizzative sono identificate in base ai contenuti e indicazioni del GDPR.

A titolo esemplificativo e non esaustivo, si elencano:

- definizione e attuazione procedura operativa per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati";

- definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante";

- definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico";

- definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali";

- definizione e attuazione procedura operativa per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalita' di accesso finalizzata all'identificazione degli incaricati";

- definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015";

- definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia:

a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;

b) le misure di ripristino in caso di "data breach";

- definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003 per i trattamenti con strumenti diversi da quelli elettronici:

a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati;

b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi;

c) le modalita' del controllo, custodia e restituzione della documentazione;

d) le modalita' del controllo degli accessi agli archivi/banche dati";

Comunicazione di una violazione dei dati personali all'interessato

Per la comunicazione di una violazione dei dati personali all'interessato, il presente PPD rinvia alla definizione e attuazione di adeguate misure organizzative e procedurali, ferma restando la disciplina del GDPR.

Deliberazione G.C. n. 165 del 25 NOV. 2020

Letto, approvato e sottoscritto:

IL SINDACO
F.to Roberto Colombo

IL SEGRETARIO GENERALE
F.to Dr.ssa Teresa La Scala

CERTIFICATO DI PUBBLICAZIONE

Il sottoscritto Segretario certifica che copia della presente deliberazione, ai sensi dell'art.124 del D. Lgs. n.267/2000 viene pubblicata all'Albo Pretorio on line di questo Comune il giorno 15 DIC. 2020
e vi rimarrà per la durata di quindici giorni consecutivi.

Lì, 15 DIC. 2020

IL SEGRETARIO GENERALE
F.to Dr.ssa Teresa La Scala

AUTENTICAZIONE

La presente copia è conforme all'originale, per uso amministrativo, ai sensi del D.P.R. 28.12.2000 n.445, art.18, composta di n. 47 fogli.

Lì 15 DIC. 2020

COMUNE DI CARUGATE (MILANO)

IL SEGRETARIO GENERALE
(Dr.ssa Teresa La Scala)

CERTIFICATO DI ESECUTIVITA'

Si certifica che il presente atto è stato pubblicato nelle forme di legge all'Albo pretorio del Comune ed E' DIVENTATO ESECUTIVO in data _____ ai sensi dell'art. 134, comma 3, del Decreto Legislativo 18/8/2000 n. 267.

IL SEGRETARIO GENERALE
F.to Dr.ssa Teresa La Scala