Comune di CANEGRATE

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.

SOMMARIO

RIFERIMENTI DOCUMENTALI

Titolo del Documento: Piano di protezione dei dati
Numero di versione: 04

Data ultimo aggiornamento 28/11/2024

Stato del documento: Approvato dal Titolare con proprio provvedimento

Estensori del documento: Comune di Canegrate (MI)

Riferimento per comunicazioni in merito al documento: Via A. Manzoni n. 1 -20039 Canegrate (MI) - Tel. 0331 463814 - PEC: comune.canegrate@pec.regione.lombardia.it

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

PREMESSA

La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale e" un diritto fondamentale. 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.

Le persone fisiche devono avere il controllo dei dati personali che li riguardano e la certezza giuridica e operativa deve essere rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorita' pubbliche. Senonche', la rapidita' dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali.

La portata della condivisione e della raccolta di dati personali e' aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorita' pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attivita'. Sempre piu' spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. La tecnologia ha trasformato l''economia e le relazioni sociali e dovrebbe facilitare ancora di piu' la libera circolazione dei dati personali all'interno dell''Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali.

Tale evoluzione ha indotto l'Unione europea ad adottare il GDPR (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 di seguito solo GDPR).

Con il GDPR e' stato richiesto agli Stati membri un quadro piu' 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.

In adeguamento al GDPR, il presente Piano di protezione dei dati personali (PPD) intende rappresentare lo strumento, il fulcro del sistema di protezione.

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.

Definizioni di cui all'art. 4 del GDPR:

- "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 di 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 strutturato 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 un 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;

- "terzo": la persona fisica o giuridica, l'autorita' pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorita' diretta del titolare o del responsabile;

- "consenso dell'interessato": qualsiasi manifestazione di volonta' libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

- "violazione dei dati personali": 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;

- "dati genetici": i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

- "dati biometrici": i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

- "dati relativi alla salute": i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

- "stabilimento principale":

a) per quanto riguarda un titolare del trattamento con stabilimenti in piu' di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalita' e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facolta' di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni e' considerato essere lo stabilimento principale;

b) con riferimento a un responsabile del trattamento con stabilimenti in piu' di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attivita' di trattamento nel contesto delle attivita' di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile e' soggetto a obblighi specifici ai sensi del presente regolamento;

- "rappresentante": la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27 del GDPR, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

- "impresa": la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attivita' economica, comprendente le societa' di persone o le associazioni che esercitano regolarmente un'attivita' economica;

- "gruppo imprenditoriale": un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

- "norme vincolanti d'impresa": le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o 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 presente 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.

OGGETTO

Il PPD individua le politiche, gli obiettivi strategici e gli standard di sicurezza per garantire la tutela dei diritti e delle liberta' fondamentali delle persone fisiche rispetto alle attivita' di trattamento dei dati personali, definendo il quadro delle MISURE DI SICUREZZA informatiche/logiche, logistiche/fisiche, organizzative e procedurali da adottare e da applicare per ridurre/eliminare il RISCHIO di violazione dei dati derivante dal trattamento.

In tale quadro, il documento disciplina, secondo i principi della UNI ISO 31000:2018, il sistema di gestione del trattamento dei dati personali e il rischio di violazione dei dati personali medesimi. La disciplina si applica ai:

1.trattamenti con strumenti elettronici;

2.trattamenti senza l'ausilio di strumenti elettronici (ad esempio: cartacei, audio, visivi e audiovisivi, ecc.).

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').

QUADRO NORMATIVO DI RIFERIMENTO

Il PPD tiene conto dei seguenti documenti:

- GDPR UE 679/2016 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;

- Legge 25 ottobre 2017, n. 163 (art.13), recante la delega per l'adeguamento della normativa nazionale alle disposizioni del GDPR (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;

- D.Lgs. n. 101/2018 di adeguamento della normativa interna al GDPR;

- Codice in materia di dati personali D.Lgs. n.196/2003 come modificato dal D.Lgs 101/2018;

- Linee guida e raccomandazioni del Garante;

- Legge 25 ottobre 2017, n. 163 (art.13), recante la delega per l'adeguamento della normativa nazionale alle disposizioni del GDPR (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;

- Dichiarazioni del gruppo di lavoro articolo 29 sulla protezione dei dati (WP29) - 14/EN;

- Linee-guida sui responsabili della protezione dei dati (RPD) - WP243 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;

- Linee-guida sul diritto alla "portabilita' dei dati" - WP242 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;

- Linee-guida per l'individuazione dell'autorita' di controllo capofila in rapporto a uno specifico titolare o responsabile del trattamento - WP244 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;

- Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonche' i criteri per stabilire se un trattamento

"possa presentare un rischio elevato" ai sensi del regolamento 2016/679 - WP248 adottate dal Gruppo di lavoro Art. 29 il 4 aprile 2017;

- Linee guida elaborate dal Gruppo Art. 29 in materia di applicazione e definizione delle sanzioni amministrative - WP253

adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017;

- Linee guida elaborate dal Gruppo Art. 29 in materia di processi decisionali automatizzati e pro lazione - WP251

Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;

- Linee guida elaborate dal Gruppo Art. 29 in materia di notifica delle violazioni di dati personali (data breach notification) - WP250 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;

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

- Allegato 1 al provvedimento n. 467 del 11 ottobre 2018 Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione di impatto

- 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 GC nr. 13 del 29/1/2025.

PERIODO DI RIFERIMENTO E MODALITA' DI AGGIORNAMENTO

Il PPD copre il periodo del triennio 2024-2026, 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;

- dirigenti/responsabili E.Q. delegati al trattamento e, loro tramite, gli incaricati del trattamento in relazione, in particolare, alle proposte di svolgere una valutazione d'impatto sulla protezione dei dati, ai contributi alla valutazione d'impatto sulla protezione dei dati e al coinvolgimento nel processo di convalida di detta valutazione;

- responsabile della sicurezza dei sistemi informativi e responsabile IT;

- responsabili del trattamento - RTD;

- responsabile Protezione dei dati - RPD.

La valutazione d'impatto sulla protezione dei dati (DPIA) e' stata svolta, all'interno dell'organizzazione, e sotto la responsabilita' del titolare, dai Dirigenti/E.Q. delegati al trattamento, avvalendosi della consulenza del RPD.

Quanto alla partecipazione degli stakeholder:

- nei casi ritenuti appropriati, proporzionati e praticabili sono state raccolte le opinioni degli interessati o dei loro rappresentanti;

- nei casi ritenuti non appropriati o sproporzionati o impraticabili e' stata, per contro, documentata la giustificazione per la mancata raccolta delle opinioni degli interessati.

CANALI, STRUMENTI E INIZIATIVE DI COMUNICAZIONE DEI CONTENUTI

Il Piano viene portato alla conoscenza dei dipendenti, dei collaboratori, della cittadinanza e dei soggetti a qualunque titolo coinvolti nell'attivita' dell'ente mediante i seguenti strumenti:

- pubblicazione sul sito istituzionale a tempo indeterminato sino a revoca o sostituzione con un PPD aggiornato;

- invio a tutto il personale dipendente tramite rete intranet;

- invio a:

 - Organismo indipendente di valutazione;

 - Revisore dei conti;

 - OOSS e RSU;

 - Commissione pari opportunita';

 - Comitato unico di Garanzia;

 - Comitato di direzione composto dai responsabili di settore dell'ente.

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).

All'esito dell'analisi, condotta anche attraverso la valutazione di impatto (DPIA), il titolare del trattamento decide, in autonomia, se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'autorita' di controllo competente per ottenere indicazioni su come gestire il rischio residuale, fermo restando che l'autorita' non ha il compito di "autorizzare" il trattamento, bensi' di indicare le misure ulteriori eventualmente da implementare a cura del titolare e puo', ove necessario, adottare tutte le misure correttive ai sensi dell'art. 58 GDPR (dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento).

LA CONFIGURAZIONE DEL SISTEMA DI PROTEZIONE COME PROTEZIONE FIN DALLA PROGETTAZIONE E PER IMPOSTAZIONE PREDEFINITA

Nel delineato sistema di protezione, l'intervento delle autorita' di controllo e' principalmente configurato come un intervento "ex post", ossia si colloca successivamente alle determinazioni assunte autonomamente dal titolare.

Tale circostanza spiega l'abolizione, a partire dal 25 maggio 2018, di alcuni istituti previsti dalla direttiva del 1995 e dal D.Lgs. n.196/ 2003, come la notifica preventiva dei trattamenti all'autorita' di controllo e il cosiddetto prior checking (o verifica preliminare di cui all'art. 17 del Codice), sostituiti da obblighi di tenuta di un registro dei trattamenti da parte del titolare/responsabile e, appunto, di effettuazione di valutazioni di impatto (DPIA) in piena autonomia.

Tenendo conto dello stato dell'arte e dei costi di adeguamento, nonche' della natura, dell'ambito di applicazione, del contesto e delle finalita' del trattamento, come anche dei rischi aventi probabilita' e gravita' diverse per i diritti e le liberta' delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, l'Ente in persona del titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte a:

- attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione;

- integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del GDPR, e tutelare i diritti degli interessati;

- garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalita' del trattamento, garantendo che non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

Il principio chiave e' sintetizzato dall'espressione inglese "data protection by default and by design" (si veda art. 25 GDPR), ossia dalla necessita' di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del GDPR e tutelare i diritti degli interessati tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le liberta' degli interessati.

Tutto questo va effettuato a monte, prima di procedere al trattamento dei dati vero e proprio e richiede, pertanto, un'analisi preventiva e un impegno applicativo che devono sostanziarsi in una serie di attivita' specifiche documentabili e dimostrabili.

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:

- il registro delle operazioni di trattamento i cui contenuti sono indicati all'art. 30 GDPR, fermo restando che il titolare o un suo delegato o il responsabile puo' inserire ulteriori informazioni se lo ritiene opportuno proprio nell'ottica della complessiva valutazione di impatto dei trattamenti svolti.

Il registro costituisce uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno dell'Ente, indispensabile per ogni valutazione e analisi del rischio. La tenuta del registro dei trattamenti non costituisce un adempimento formale bensi' parte integrante di un sistema di corretta gestione dei dati personali.

A fini della istituzione e della tenuta del registro, il titolare del trattamento compie e tiene costantemente aggiornata:

- un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche.

Accountability: Misure di sicurezza

Accountability: Misure di sicurezza

Il principio di responsabilizzazione richiede altresi' che, effettuata la ricognizione dei trattamenti, il titolare valuti l'adeguato livello di sicurezza da adottare, tendo conto in special modo dei rischi 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. Sul punto il RGDP prevede che il titolare del trattamento e il responsabile del trattamento:

- effettuino una valutazione di impatto del trattamento sulla sicurezza dei dati, posto che 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;

- 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, mettano 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.

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, 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 minime di sicurezza informatica generate da AGID per la sicurezza nel trattamento dei dati digitali.

Accountability: Notifica delle violazioni di dati personali

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.

La notifica all'autorita' dell'avvenuta violazione non e' obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al titolare.

Se la probabilita' di tale rischio e' elevata, e' necessario informare della violazione anche gli interessati, sempre "senza ingiustificato ritardo" ferme restando le eccezioni costituite dalle circostanze indicate al paragrafo 3 dell'art. 34 del GDPR.

I contenuti:

- della notifica all'autorita';

- della comunicazione agli interessati,

indicati, in via non esclusiva, agli artt. 33 e 34 del GDPR e dalla normativa interna di adeguamento.

In conclusione, il titolare del trattamento e' tenuto, in ogni caso, a documentare le violazioni di dati personali subite, anche se non notifcate all'autorita' di controllo e non comunicate agli interessati, nonche' le relative circostanze e conseguenze e i provvedimenti adottati. In forza di questo obbligo di documentazione, il titolare di trattamento e' tenuto a:

- adottare le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuto a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

Accountability: Responsabile della protezione dei dati

Accountability: Responsabile della protezione dei dati

Anche la designazione di un "responsabile della protezione dati" (RPD/DPO), quale figura indipendente, autorevole, dotata di competenze manageriali e tenuta al segreto d'ufficio, riflette l'approccio responsabilizzante che e' proprio del GDPR, essendo finalizzata a facilitare l'adeguamento del GDPR da parte del titolare e del responsabile. Non e' un caso, il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento nello svolgimento dei compiti affidati, che sono:

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonche' ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR nonche' da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) sorvegliare l'osservanza del 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;

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;

- obblighi di legge cui e' soggetto il titolare;

- interesse pubblico o esercizio di pubblici poteri;

- interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati.

In definitiva, il trattamento e' lecito, ai sensi dell'art. 6 par. 1 del GDPR, solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o piu' specifiche finalita';

b) il trattamento e' necessario all'esecuzione di un contratto di cui l'interessato e' parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento e' necessario per adempiere un obbligo legale al quale e' soggetto il titolare del trattamento;

d) il trattamento e' necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

e) il trattamento e' necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui e' investito il titolare del trattamento;

f) il trattamento e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore.

La lettera f) non si applica al trattamento di dati effettuato dalle Autorita' pubbliche nell'esecuzione dei loro compiti.

Relativamente alla lett. a) e al consenso, la disciplina del GDPR prevede che:

- se il consenso dell'interessato e' prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso e' presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento e' vincolante;

- l'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceita' del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato e' informato di cio'. Il consenso e' revocato con la stessa facilita' con cui e' accordato;

- nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualita', tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

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.

La base giuridica su cui si fonda il trattamento dei dati deve essere stabilita:

- dal diritto dell'Unione;

- dal diritto dello Stato membro cui e' soggetto il titolare del trattamento.

La finalita' del trattamento e' determinata:

- in tale base giuridica;

- o e' necessaria, per quanto riguarda il trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui e' investito il titolare del trattamento.

Tale base giuridica potrebbe contenere disposizioni specifiche per adeguare l'applicazione delle norme del GDPR, tra cui:

- le condizioni generali relative alla liceita' del trattamento da parte del titolare del trattamento;

- le tipologie di dati oggetto del trattamento; gli interessati;

- i soggetti cui possono essere comunicati i dati personali e le finalita' per cui sono comunicati;

- le limitazioni della finalita', i periodi di conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto, quali quelle per altre specifiche situazioni di trattamento di cui al capo IX.

Il diritto dell'Unione o degli Stati membri persegue un obiettivo di interesse pubblico ed e' proporzionato all'obiettivo legittimo perseguito.

Laddove il trattamento per una finalita' diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una societa' democratica per la salvaguardia degli obiettivi di

cui all'articolo 23, paragrafo 1 GDPR, al fine di verificare se il trattamento per un'altra finalita' sia compatibile con la finalita' per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro:

a) di ogni nesso tra le finalita' per cui i dati personali sono stati raccolti e le finalita' dell'ulteriore trattamento previsto;

b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento;

c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10;

d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;

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.

Se il trattamento comporta processi decisionali automatizzati (anche la profilazione), l'informativa deve specificarlo e deve indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato.

Tempi dell'informativa
Nel caso di dati personali non raccolti direttamente presso l'interessato:
- l'informativa deve essere fornita entro un termine ragionevole che non puo' superare 1 mese dalla raccolta, oppure al momento della comunicazione (NON della registrazione) dei dati (a terzi o all'interessato).

Modalita' dell'informativa
L'informativa deve avere forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile.
Occorre utilizzare un linguaggio chiaro e semplice, e per i minori occorre prevedere informative idonee.

L'informativa e' data, in linea di principio, per iscritto e preferibilmente in formato elettronico soprattutto nel contesto di servizi online anche se sono ammessi "altri mezzi", potendo essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra.

Il GDPR ammette, soprattutto, l'utilizzo di icone per presentare i contenuti dell'informativa in forma sintetica, ma solo "in combinazione" con l'informativa estesa e conformemente ai modelli di icone definite prossimamente dalla Commissione europea.

In caso di dati personali raccolti da fonti diverse dall'interessato, va valutato caso per caso se la prestazione dell'informativa agli interessati comporti uno sforzo sproporzionato.

L'informativa deve essere fornita all'interessato prima di effettuare la raccolta dei dati.

Se i dati non sono raccolti direttamente presso l'interessato, l'informativa deve comprendere anche le categorie dei dati personali oggetto di trattamento.

In tutti i casi, il titolare deve specificare:

- la propria identita';

- quella dell'eventuale rappresentante nel territorio italiano;

- le finalita' del trattamento;

- i diritti degli interessati (compreso il diritto alla portabilita' dei dati);

- se esiste un responsabile del trattamento e la sua identita';

- 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.

L'esercizio dei diritti e', in linea di principio, gratuito per l'interessato, ma possono esservi eccezioni. Il titolare ha il diritto di chiedere informazioni necessarie a identificare l'interessato, e quest'ultimo ha il dovere di fornirle, secondo modalita' idonee. Sono ammesse deroghe ai diritti riconosciuti dal GDPR, ma solo sul fondamento di disposizioni normative nazionali, ai sensi dell'articolo 23 nonche' di altri articoli relativi ad ambiti specifici.

Il termine per la risposta all'interessato e', per tutti i diritti (compreso il diritto di accesso):

- 1 mese, estendibili fino a 3 mesi in casi di particolare complessita'; il titolare o un suo delegato deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego.

Spetta al titolare valutare la complessita' del riscontro all'interessato e stabilire l'ammontare dell'eventuale contributo da chiedere all'interessato, ma soltanto se si tratta di richieste manifestamente infondate o eccessive (anche ripetitive) (art. 12.5), a differenza di quanto prevedono gli artt. 9, comma 5, e 10, commi 7 e 8, del Codice, ovvero se sono chieste piu' "copie" dei dati personali nel caso del diritto di accesso (art. 15, paragrafo 3); in quest'ultimo caso il titolare o un suo delegato deve tenere conto dei costi amministrativi sostenuti.

Il riscontro all'interessato di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilita'; puo' essere dato oralmente solo se cosi' richiede l'interessato stesso (art. 12, paragrafo 1; si veda anche art. 15, paragrafo 3).

La risposta fornita all'interessato non deve essere solo "intelligibile", ma anche concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.

Diritto di accesso

Il presente PPD tiene conto della disciplina del GDPR in tema di diritto di accesso secondo la quale l'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) le finalita' del trattamento;

b) le categorie di dati personali in questione;

c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;

d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non e' possibile, i criteri utilizzati per determinare tale periodo;

e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;

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;

d) i dati personali sono stati trattati illecitamente;

e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui e' soggetto il titolare del trattamento;

f) i dati personali sono stati raccolti relativamente all'offerta di servizi della societa' dell'informazione di cui all'articolo 8, paragrafo 1.

Il titolare, se ha reso pubblici dati personali ed e' obbligato a cancellarli ai sensi del paragrafo 1, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:

a) per l'esercizio del diritto alla liberta' di espressione e di informazione;

b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui e' soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui e' investito il titolare del trattamento;

c) per motivi di interesse pubblico nel settore della sanita' pubblica in conformita' dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;

d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;

e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni, 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 limitazione
Il presente PPD tiene conto della disciplina del GDPR in tema di diritto alla limitazione e di seguito indicata.

L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti condizioni:

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.

Nell'esercitare i propri diritti relativamente alla portabilita' dei dati, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.

L'esercizio del diritto alla portabilita' lascia impregiudicato il diritto alla cancellazione. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui e' investito il titolare del trattamento.

Il diritto alla portabilita' non deve ledere i diritti e le liberta' altrui.

Diritto di opposizione e processo decisionale automatizzato relativo alle persone

L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f) del GDPR, compresa la profilazione sulla base di tali disposizioni.

Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle liberta' dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. Il diritto di cui ai paragrafi 1 e 2 e' esplicitamente portato all'attenzione dell'interessato ed e' presentato chiaramente e separatamente da qualsiasi altra informazione al piu' tardi al momento della prima comunicazione con l'interessato.

Nel contesto dell'utilizzo di servizi della societa' dell'informazione e fatta salva la direttiva 2002/58/CE, l'interessato puo' esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche.

Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1 GDPR, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo se il trattamento e' necessario per l'esecuzione di un compito di interesse pubblico.

Raccomandazioni del Garante

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

- Modalita' per l'esercizio dei diritti

E' opportuno che il titolare di trattamento adotti le misure tecniche e organizzative eventualmente necessarie per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati, che - a differenza di quanto attualmente previsto - dovra' avere per impostazione predefinita forma scritta (anche elettronica). Potranno risultare utili le indicazioni fornite dal Garante nel corso degli anni con riguardo all'intelligibilita' del riscontro fornito agli interessati e alla completezza del riscontro stesso. Quanto alla definizione eventuale di un contributo spese da parte degli interessati, che il regolamento rimette al titolare del trattamento, va tenuto presente che l'Autorita' intende valutare l'opportunita' di definire linee-guida specifiche, a cui si rinvia.

- 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, paragrafo 9, e art. 96). Restano valide, conseguentemente, le autorizzazioni nazionali sinora emesse dal Garante successivamente a tali decisioni di adeguatezza della Commissione;

- in assenza di decisioni di adeguatezza della Commissione, garanzie adeguate di natura contrattuale o pattizia che devono essere fornite dai titolari coinvolti (fra cui le norme vincolanti d'impresa - BCR, e clausole contrattuali modello): in mancanza di una decisione di adeguatezza, il titolare del trattamento o il responsabile del trattamento puo' trasferire, , ai sensi dell'art. 46 GDPR, dati personali verso un paese terzo o un'organizzazione internazionale solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi;

- in assenza di ogni altro presupposto, utilizzo di deroghe al divieto di trasferimento applicabili in specifiche situazioni: in mancanza di una decisione di adeguatezza, o di garanzie adeguate, comprese le norme vincolanti d'impresa, e' ammesso il trasferimento o un complesso di trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale soltanto se si verifica una delle condizioni indicate nell'art. 49 GDPR.

Il GDPR, inoltre:

- consente di ricorrere anche a codici di condotta ovvero a schemi di certificazione per dimostrare le "garanzie adeguate" previste dall'art. 46. Cio' significa che i titolari o i responsabili del trattamento stabiliti in un Paese terzo potranno far valere gli impegni sottoscritti attraverso l'adesione al codice di condotta o allo schema di certificazione, ove questi disciplinino anche o esclusivamente i trasferimenti di dati verso Paesi terzi, al fine di legittimare tali trasferimenti. Tuttavia (si vedano art. 40, paragrafo 3, e art. 42, paragrafo 2), tali titolari dovranno assumere, inoltre, un impegno vincolante mediante uno specifico strumento contrattuale o un altro strumento che sia giuridicamente vincolante e azionabile dagli interessati;

- vieta trasferimenti di dati verso titolari o responsabili in un Paese terzo sulla base di decisioni giudiziarie o ordinanze amministrative emesse da autorita' di tale Paese terzo, a meno dell'esistenza di accordi internazionali in particolare di mutua assistenza giudiziaria o analoghi accordi fra gli Stati (si veda art. 48). Si potranno utilizzare, tuttavia, gli altri presupposti e in particolare le deroghe previste per situazioni specifiche di cui all'art. 49. A tale riguardo, si deve ricordare che il regolamento chiarisce come sia lecito trasferire dati personali verso un Paese terzo non adeguato "per importanti motivi di interesse pubblico", in deroga al divieto generale, ma deve trattarsi di un interesse pubblico riconosciuto dal diritto dello Stato membro del titolare o dal diritto dell'Ue (si veda art. 49, paragrafo 4) e, dunque, non puo' essere fatto valere l'interesse pubblico dello Stato terzo ricevente;

- fissa i requisiti per l'approvazione delle norme vincolanti d'impresa e i contenuti obbligatori di tali norme. L'elenco indicato al riguardo nel paragrafo 2 dell'art. 47 non e' esaustivo e, pertanto, potranno essere previsti dalle autorita' competenti, a seconda dei casi, requisiti ulteriori. Ad ogni modo, l'approvazione delle norme vincolanti d'impresa dovra' avvenire esclusivamente attraverso il meccanismo di coerenza di cui agli artt. 63-65 del regolamento - ossia, e' previsto in ogni caso l'intervento del Comitato europeo per la protezione dei dati (si veda art. 64, paragrafo 1, lettera d)).

In forza della descritta disciplina, in primo luogo, viene meno il requisito dell'autorizzazione nazionale. Cio' significa che il trasferimento verso un Paese terzo "adeguato" ai sensi della decisione assunta in futuro dalla Commissione, ovvero sulla base di clausole contrattuali modello, debitamente adottate, o di norme vincolanti d'impresa approvate attraverso la specifica procedura di cui all'art. 47 del GDPR potra' avere inizio senza attendere l'autorizzazione nazionale del Garante - a differenza di quanto in passato previsto dall'art. 44 del D.Lgs.196/2003.

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.

PARTE III
CONTESTO, SOGGETTI RESPONSABILI , SICUREZZA E DOCUMENTAZIONE DEL SISTEMA DI PROTEZIONE

IL CONTESTO DEL SISTEMA DI PROTEZIONE

La descrizione riassuntiva del contesto, tenendo conto della sintetica descrizione del trattamento e del flusso informativo, ha lo scopo di delineare il complessivo stato di fatto e di diritto nel quale si inserisce il trattamento, si a con riferimento al contesto esterno che con riferimento al contesto interno.
Per quanto concerne il contesto interno, tiene conto in particolare:

- degli atti di programmazione e pianificazione generale dell'Ente - disposizioni e atti generali (direttive, circolari, programmi e istruzioni) - organizzazione e articolazione degli uffici (organigramma e funzionigramma) - mappatura dell'attivita' (processi e procedimenti) - inventario dei beni (mobili e immobili) e mappatura delle risorse strumentali - elenco di consulenti e collaboratori - atti e provvedimenti degli organi di indirizzo e gestionali - catalogo di dati, metadati, banche dati - disciplina particolare dell'attivita' oggetto di trattamento, inclusa la Lex specialis;

- dei soggetti che effettuano il trattamento e dei soggetti che sono autorizzati ad accedere ai locali fuori dall'orario di servizio.

I SOGGETTI E LE RESPONSABILITA'

Titolare del trattamento

Il titolare e' la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo a cui competono, anche unitamente ad altro titolare, le decisioni in ordine:
- alle finalita';

- alle modalita' del trattamento di dati personali;

- agli strumenti utilizzati;

ivi compreso il profilo della sicurezza.

Le decisioni del titolare in ordine a quanto sopra tengono conto dei:

- principi applicabili al trattamento di dati diversi da quelli appartenenti a particolari categorie e giudiziari: il trattamento riguardante dati diversi da quelli appartenenti a particolari categorie e giudiziari e' consentito soltanto per lo svolgimento delle funzioni istituzionali, anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente. La comunicazione ad altri soggetti pubblici e' ammessa quando e' prevista da una norma di legge o di regolamento. In

mancanza di tale norma la comunicazione e' ammessa quando e' comunque necessaria per lo svolgimento di funzioni istituzionali ai sensi dell'art. 2-ter de D.Lgs 196/2003. 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 appartenenti a particolari categorie disciplinate dall'art. 9 del GDPR: il trattamento d di tali dati 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. L'art. 2-sexies del D.Lgs 196/2003 definisce ed elenca i procedimenti e le condizioni che vengono considerati dal legislatore trattamenti di rilevante interesse pubblico che rendono lecito il trattamento dei dati appartenenti a particolari categorie.

- 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 di Regolamento che specifichino le finalita' di rilevante interesse pubblico del trattamento, i tipi di dati trattati e di 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. L'art. 2-octies del d.Lgs 196/2003 definisce gli ambiti in cui il trattamento dei dati giudiziari puo' essere autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento.

- 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 assicurare che i dati sensibili e giudiziari siano indispensabili rispetto agli obblighi e ai compiti attribuiti, e' necessario valutare specificamente il rapporto tra i dati e gli adempimenti. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione e' prestata per la verifica dell'indispensabilita' dei dati sensibili e giudiziari riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni o gli adempimenti. I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi e' autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessita'. I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalita' che non richiedono il loro utilizzo. I medesimi dati sono trattati con le modalita' sopra indicate anche quando sono tenuti in elenchi, registri o banche di dati senza l'ausilio di strumenti elettronici. I dati idonei a rivelare lo stato di salute non possono essere diffusi. Rispetto ai dati sensibili e giudiziari indispensabili, e' lecito effettuare unicamente le operazioni di trattamento indispensabili per il

perseguimento delle finalita' per le quali il trattamento e' consentito, anche quando i dati sono raccolti nello svolgimento di compiti di vigilanza, di controllo o ispettivi. I dati sensibili e giudiziari non possono essere trattati nell'ambito di test psicoattitudinali volti a definire il profilo o la personalita' dell'interessato. Le operazioni di raffronto tra dati sensibili e giudiziari, nonche' i trattamenti di dati sensibili e giudiziari per la definizione di profili e della personalita' dell'interessato, sono effettuati solo previa annotazione scritta dei motivi. In ogni caso, le operazioni e i trattamenti di cui ai test psicoattitudinali volti a definire il profilo o la personalita' dell'interessato, se effettuati utilizzando banche di dati di diversi titolari, nonche' la diffusione dei dati sensibili e giudiziari, sono ammessi solo se previsti da espressa disposizione di legge.

Contitolari del trattamento

Allorche' due o piu' titolari del trattamento determinano congiuntamente le finalita' e i mezzi del trattamento, essi sono contitolari del trattamento.

I contitolari determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilita' in merito all'osservanza degli obblighi derivanti dal presente GDPR, con particolare riguardo:

- all'esercizio dei diritti dell'interessato;

- alle rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14 GDPR, a meno che e nella misura in cui le rispettive responsabilita' siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti.

Tale accordo deve designare un punto di contatto dei contitolari per gli interessati. L'accordo riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo e' messo a disposizione dell'interessato. Indipendentemente dalle disposizioni dell'accordo, l'interessato puo' esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun titolare del trattamento.

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;

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 del GDPR, 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 PPD o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

Il responsabile effettua il trattamento attenendosi alle condizioni stabilite nel contratto o atto giuridico, e alle istruzioni impartite dal titolare, il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di legge e regolamento, delle proprie istruzioni e di quanto stabilito nel contratto o atto giuridico.

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 PPD. 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 del GDPR o a un meccanismo di certificazione approvato di cui all'articolo 42 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.

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

Nel GDPR e nel D.Lgs 196/2003, si distinguono il soggetto designato al trattamento dei dati (Dirigente/E.Q.) dal soggetto autorizzato.

a) Soggetto Designato

Il Titolare conferisce i sotto indicati compiti e funzioni, e i correlati poteri, mediante apposito provvedimento di delega o di nomina, da adottarsi secondo il proprio ordinamento ai:

- dirigenti/ titolari E.Q.

Nel suddetto provvedimento, il Titolare deve informare ciascun dirigente/E.Q., delle responsabilita' che gli sono affidate in relazione a quanto disposto dal Codice, dal GDPR e dal presente Regolamento, specificando nell'atto compiti funzioni e potere.

Ciascun dirigente/titolare E.Q., nell'espletamento dei compiti, funzioni e poteri delegati o per i quali ha ricevuto la nomina, collabora con il Titolare al fine di:

- comunicare tempestivamente, l'inizio di ogni nuovo trattamento, la cessazione o la modifica dei trattamenti in atto, nonche' ogni notizia rilevante ai fini dell'osservanza degli obblighi dettati dagli articoli da 32 a 36 del GDPR riguardanti l'adozione di misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio; la notificazione di una violazione dei dati personali al Garante privacy; la comunicazione di una violazione dei dati personali all'interessato; la redazione della valutazione d'impatto sulla protezione dei dati; la consultazione preventiva;

- predisporre le informative previste e verificarne il rispetto e fornire le informazioni necessarie per l'aggiornamento del registro dei trattamenti;

- designare gli incaricati del trattamento, e fornire loro specifiche istruzioni;

- rispondere alle istanze degli interessati secondo quanto stabilito dal Codice e stabilire modalita' organizzative volte a facilitare l'esercizio del diritto di accesso dell'interessato e la valutazione del bilanciamento degli interessi in gioco;

- garantire che tutte le misure di sicurezza riguardanti i dati del Titolare siano applicate all'interno della struttura organizzativa dell'Ente ed all'esterno, qualora agli stessi abbiano accesso da parte di soggetti terzi quali responsabili del trattamento;

- informare il Titolare del trattamento, senza ingiustificato ritardo, della conoscenza dell'avvenuta violazione dei dati personali.

Ciascun dirigente/E.Q. risponde al Titolare di ogni violazione o mancata attivazione di quanto dettato dalla normativa vigente e della mancata attuazione delle misure di sicurezza.

I dirigenti/E.Q. sono destinatari degli interventi di formazione di aggiornamento.

b) Incaricati del Trattamento dei dati

Gli incaricati del trattamento sono le persone fisiche, dipendenti del Titolare, designati da ciascun dirigente/E.Q., incaricati di svolgere le operazioni di trattamento dei dati personali di competenza con l'indicazione specifica dei compiti, dell'ambito di trattamento consentito, e delle modalita'.

La designazione dell'incaricato al trattamento dei dati personali e' di competenza del dirigente/E.Q.; la nomina e' effettuata per iscritto e individua specificatamente i compiti spettanti all'incaricato e le modalita' cui egli deve attenersi per l'espletamento degli stessi e l'ambito del trattamento consentito.

A prescindere dalla nomina, si considera tale anche la documentata preposizione della persona fisica ad un'unita' per la quale risulti individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unita' medesima. Per effetto di tale disposizione, ogni dipendente preposto ad un determinato ufficio/servizio, tenuto ad effettuare operazioni di trattamento nell'ambito di tale servizio, e' da considerare incaricato ai sensi dell'art. 2-quaterdecies del Codice nonche' ai sensi degli artt. 4 comma 10 e art. 29 del GDPR.

Gli incaricati devono comunque ricevere idonee ed analitiche istruzioni, anche per gruppi omogenei di funzioni, riguardo le attivita' sui dati affidate e gli adempimenti a cui sono tenuti.

Gli incaricati collaborano con il Titolare ed il dirigente/E.Q. segnalando eventuali situazioni di rischio nel trattamento dei dati e fornendo ogni informazione necessaria per l'espletamento delle funzioni di controllo.

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.

Responsabile della protezione dei dati (RPD/DPO)
Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal GDPR.

Il RPD/DPO:

- puo' svolgere altri compiti e funzioni a condizione che tali compiti e funzioni non diano adito a un conflitto di interessi;

- e' tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti.

Il responsabile della protezione dei dati e' incaricato dei seguenti compiti:

- informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonche' ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente GDPR nonche' da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

- 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) . 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 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 del GDPR 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.

Codici di condotta

Il presente PPD tiene conto che gli Stati membri, le autorita' di controllo, il comitato e la Commissione incoraggiano:

- l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del presente GDPR, in funzione delle specificita' dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese.

Le associazioni e gli altri organismi rappresentanti le categorie del titolare del trattamento o responsabili del trattamento:

- possono elaborare i codici di condotta, modificarli o prorogarli, allo scopo di precisare l'applicazione del presente GDPR, ad esempio relativamente a:

a) il trattamento corretto e trasparente dei dati;

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.

Il titolare del trattamento o il responsabile del trattamento che sottopone il trattamento effettuato al meccanismo di certificazione fornisce all'organismo di certificazione di cui all'articolo 43 del GDPR o, ove applicabile, all'autorita' di controllo competente tutte le informazioni e l'accesso alle attivita' di trattamento necessarie a espletare la procedura di certificazione.

La certificazione e' rilasciata al titolare del trattamento o responsabile del trattamento per un periodo massimo di tre anni e puo' essere rinnovata alle stesse condizioni purche' continuino a essere soddisfatti i requisiti pertinenti. La certificazione e' revocata, se del caso, dagli organismi di certificazione di cui all'articolo 43 del GDPR o dall'autorita' di controllo competente, a seconda dei casi, qualora non siano o non siano piu' soddisfatti i requisiti per la certificazione.

Notifica di una violazione dei dati personali all'Autorita' di controllo

In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorita' di controllo competente a norma dell'articolo 55 del GDPR:
- 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.

Qualora la notifica all'autorita' di controllo non sia effettuata entro 72 ore, e' corredata dei motivi del ritardo.

Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

La notifica deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonche' le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere piu' informazioni;

c) descrivere le probabili conseguenze della violazione dei dati personali;

d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

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 organizzazione e di gestione del rischio di violazione dei dati personali (SOGDP) sono documentati almeno da:

Piano protezione dati -PPD;

Registri delle attivita' e delle categorie dei trattamenti;

Legende identificativi (ID) utilizzati nel PPD e negli allegati

Mappa struttura organizzativa;

Mappa dei soggetti del sistema di protezione, inclusi i soggetti esterni a cui e' affidato il trattamento dei dati;

Mappa dei luoghi;

Schede di ricognizione dei trattamenti/Indice-Mappa dei trattamenti;

Mappa hardware;

Mappa software, con indicazione degli archivi e delle banche dati elettroniche;

Mappa rischi e motivazioni stima;

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

Schede di valutazione di impatto (DPIA) per i trattamenti a rischio elevato;

Schede di sintesi della valutazione di impatto sulla protezione dei dati (DPIA) da pubblicare sul sito web dell'Ente;

Mappa delle misure di sicurezza logistiche/fisiche;

Mappa delle misure di sicurezza informatiche/logiche;

Mappa delle misure di sicurezza organizzative;

Mappa delle misure di sicurezza e procedurali;

Elenco delle misure di sicurezza correlate all'indice dei trattamenti e suddivise per uffici;

Atti di delega al trattamento dei dati;

Atti di nomina degli incaricati;

Piano di formazione in materia di diritti e di liberta' delle persone e di protezione dei dati personali per i soggetti autorizzati al trattamento e per incaricati del back up;

Misure minime ITC e relativa implementazione adottate entro il 31 dicembre 2017.

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 31.000:2018, 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.

g) La gestione del rischio e' "su misura". La gestione del rischio e' in linea con il contesto esterno ed interno e con il profilo di rischio dell'organizzazione.

h) La gestione del rischio tiene conto dei fattori umani e culturali. Nell'ambito della gestione del rischio individua capacita', percezioni e aspettative delle persone esterne ed interne che possono facilitare o impedire il raggiungimento degli obiettivi dell'organizzazione.

i) La gestione del rischio e' trasparente e inclusiva. Il coinvolgimento appropriato e tempestivo dei portatori d'interesse e, in particolare, dei responsabili delle decisioni, a tutti i livelli dell'organizzazione, assicura che la gestione del rischio rimanga pertinente ed aggiornata. Il coinvolgimento, inoltre, permette che i portatori d'interesse siano opportunamente rappresentati e che i loro punti di vista siano presi in considerazione nel definire i criteri di rischio.

j) La gestione del rischio e' dinamica. La gestione del rischio e' sensibile e risponde al cambiamento continuamente. Ogni qual volta accadono eventi esterni ed interni, cambiano il contesto e la conoscenza, si attuano il monitoraggio ed il riesame, emergono nuovi rischi, alcuni rischi si modificano ed altri scompaiono.

k) La gestione del rischio favorisce il miglioramento continuo dell'organizzazione. Le organizzazioni dovrebbero sviluppare ed attuare strategie per migliorare la maturita' della propria gestione del rischio insieme a tutti gli altri aspetti della propria organizzazione.

La gestione di rischi derivanti dal trattamento sulla protezione dei dati personali viene condotta attraverso le fasi di:

- analisi del rischio, quale fase del processo di gestione nella quale viene definito il contesto esterno e interno, di natura organizzativa e gestionale;

- valutazione del rischio, quale fase del processo di gestione del rischio che identifica, analizza e pondera il rischio medesimo;

- trattamento del rischio.

GESTIONE DEL RISCHIO SECONDO LA NORMA UNI ISO 31.000: FASE DELLA ANALISI

Contesto interno organizzativo

L'articolo 35 del GDPR fa riferimento al possibile rischio elevato "per i diritti e le liberta' delle persone fisiche".

Come indicato nella dichiarazione del gruppo di lavoro articolo 29 sulla protezione dei dati sul ruolo di un approccio basato sul rischio nei quadri giuridici in materia di protezione dei dati, il riferimento a "diritti e liberta'" degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche

altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.

I documenti facenti parte del sistema di organizzazione e di gestione del rischio di violazione dei dati personali (SOGDP) , 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

L'organigramma privacy dell'Ente e' indicato nella MAPPA ORGANIGRAMMA PRIVACY facente parte del sistema di organizzazione e di gestione del rischio di violazione dei dati personali (SOGDP), e corrisponde alle funzioni istituzionali e ai compiti assegnati a ciascuna struttura.

La MAPPA DEI LUOGHI facente parte del sistema di organizzazione e di gestione del rischio di violazione dei dati personali (SOGDP), 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: Comune di Canegrate

Sede: Via A. Manzoni n. 1 -20039 Canegrate (MI)

Punti di contatto: Tel. 0331 463814 - PEC: comune.canegrate@pec.regione.lombardia.it

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: Modica Matteo

Sede: Via A. Manzoni n. 1 -20039 Canegrate (MI)

Punti di contatto: Tel. 0331 463814 - PEC: comune.canegrate@pec.regione.lombardia.it

Soggetti: Contitolari del trattamento

La MAPPA DEI SOGGETTI facente parte del sistema di organizzazione e di gestione del rischio di violazione dei dati personali (SOGDP) , riepiloga, con riferimento a tutti i trattamenti effettuati dall'Ente, i casi in cui il titolare, sopra indicato, e uno o piu' altri titolari del trattamento determinano congiuntamente le finalita' e i mezzi del trattamento.

I contitolari determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilita' in merito all'osservanza degli obblighi derivanti dal presente GDPR, con particolare riguardo:

- all'esercizio dei diritti dell'interessato;

- alle rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilita' siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti.

Tale accordo deve designare un punto di contatto per gli interessati.

Soggetti: Responsabili del trattamento e sub-responsabili

La MAPPA dei soggetti facente parte del sistema di organizzazione e di gestione del rischio di violazione dei dati personali (SOGDP), riepiloga, con riferimento a tutti i trattamenti effettuati dall'Ente, i casi in cui un trattamento debba essere effettuato per conto del titolare del trattamento, da un responsabile del trattamento che presenti garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato.

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 vincoli il responsabile del trattamento al titolare del trattamento e che stipuli 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 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;

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.

Soggetti: Incaricati

Nel GDPR e nel D.Lgs 196/2003, si distinguono il soggetto designato al trattamento dei dati (Dirigente/E.Q.) dal soggetto incaricato.

a) Il Soggetto Designato. Il Titolare designa i soggetti responsabili degli Uffici o dei servizi (Dirigenti e/o E.Q.), conferendo loro compiti e funzioni, e i correlati poteri, propri del titolare mediante apposito provvedimento di delega o di nomina e riferiti all'Ufficio o Area di cui sono Responsabili.

b)I soggetti Designati, in forza della delega ricevuta dal Legale Rappresentante del l'Ente Titolare, ai sensi dell'art. 2-quaterdecies del D.Lgs 196/2003 nonche' ai sensi degli artt. 4 comma 10 e art. 29 del GDPR, autorizzano le persone fisiche che operano sotto la direzione dei soggetti Designati, nominandoli soggetti incaricati e specificando nell'atto di nomina scritto i compiti spettanti all'incaricato e le modalita' cui egli deve attenersi per l'espletamento degli stessi e l'ambito del trattamento consentito

La MAPPA dei soggetti, facente parte del sistema di organizzazione e di gestione del rischio di violazione dei dati personali (SOGDP) riepiloga con riferimento a tutti i trattamenti effettuati dall'Ente, l'Elenco dei casi in cui un il responsabile del trattamento, o chiunque agisca sotto la sua autorita' o sotto quella del titolare del trattamento, che abbia accesso a dati personali puo' trattare tali dati previa istruzione.

Soggetti: Responsabile della protezione dati (RPD/DPO)

La MAPPA dei soggetti, facente parte del sistema di organizzazione e di gestione del rischio di violazione dei dati personali (SOGDP), riepiloga i dati del Responsabile della protezione dei dati.

Soggetti: Titolare del trattamento

Denominazione	Sede	Punti di contatto
Comune di Canegrate	**Via A. Manzoni n. 1 -20039 Canegrate (MI)**	**Tel. 0331 463814 - PEC: comune.canegrate@pec.regione.lombardia.it**

Soggetti: Legale rappresentante del titolare del trattamento

Anagrafica	Sede	Punti di contatto
Modica Matteo	**Via A. Manzoni n. 1 -20039 Canegrate (MI)**	**Tel. 0331 463814 - PEC: comune.canegrate@pec.regione.lombardia.it**

Contesto interno gestionale e operativo
L'Ente ha adottato le Schede gia' predisposte dal Garante della Privacy in relazione ai procedimenti della pubblica amministrazione per il trattamento dei dati sensibili e giudiziari. Sono state individuate, analiticamente, le operazioni che possono spiegare effetti maggiormente significativi per l'interessato tra quelle effettuate da questo Ente, in particolare le operazioni di interconnessione, raffronto tra banche di dati gestite da diversi il titolare, oppure con altre informazioni sensibili e giudiziarie detenute dal medesimo titolare del trattamento, di comunicazione a terzi, nonche' di diffusione.

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

Schede di ricognizione dei trattamenti

Fanno parte del sistema di organizzazione e di gestione del rischio di violazione dei dati personali (SOGDP), 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, facente parte del sistema di organizzazione e di gestione del rischio di violazione dei dati personali (SOGDP), 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, facente parte del sistema di organizzazione e di gestione del rischio di violazione dei dati personali (SOGDP), 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, facente parte del sistema di organizzazione e di gestione del rischio di violazione dei dati personali (SOGDP), 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, facente parte del sistema di organizzazione e di gestione del rischio di violazione dei dati personali (SOGDP), 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 organizzazione e di gestione del rischio di violazione dei dati personali (SOGDP) le Schede di determinazione preliminare della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del GDPR (UE) 2016/679.

Si tratta di documenti:

- conformi alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del GDPR (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017;

- necessari per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al GDPR.

Schede di valutazione di impatto sulla protezione dei dati (DPIA)

Fanno parte del sistema di protezione le Schede di valutazione di impatto sulla protezione dei dati (DPIA) che esaminano i trattamenti che presentano rischi elevati.

Si tratta di documenti:

- redatti conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del GDPR (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017;

- necessari per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al GDPR.

Fanno parte del sistema di protezione sistema di organizzazione e di gestione del rischio di violazione dei dati personali (SOGDP) le Schede di sintesi della valutazione di impatto sulla protezione dei dati (DPIA) da pubblicare sul sito web dell'Ente, laddove tale obbligo sia previsto dal SOGDP.

Mappa misure di sicurezza logistiche/fisiche

Fa parte integrante e sostanziale del sistema di organizzazione e di gestione del rischio di violazione dei dati personali (SOGDP) la MAPPA delle misure di sicurezza logistiche/fisiche

Mappa misure di sicurezza informatiche/logiche

Fa parte integrante e sostanziale del sistema di organizzazione e di gestione del rischio di violazione dei dati personali (SOGDP) la MAPPA delle misure di sicurezza informatiche/logiche.

Mappa misure di sicurezza organizzative

Fa parte integrante e sostanziale del sistema di organizzazione e di gestione del rischio di violazione dei dati personali (SOGDP) la MAPPA delle misure di sicurezza organizzative.

Mappa misure di sicurezza procedurali

Fa parte integrante e sostanziale del sistema di sistema di organizzazione e di gestione del rischio di violazione dei dati personali (SOGDP) la MAPPA delle misure di sicurezza procedurali.

Elenco misure di sicurezza

Fa parte integrante e sostanziale del sistema di organizzazione e di gestione del rischio di violazione dei dati personali (SOGDP) l'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 organizzazione e di gestione del rischio di violazione dei dati personali (SOGDP):

- 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 organizzazione e di gestione del rischio di violazione dei dati personali (SOGDP):

- atti di delega al trattamento dei dati;

- atti di nomina degli incaricati.

Costituiscono parte del sistema di organizzazione e di gestione del rischio di violazione dei dati personali (SOGDP), quand'anche non fisicamente allegati al presente documento, i seguenti ulteriori documenti:

- elenco misure minime ITC e relative implementazioni individuate dal AGID, ed adeguate in relazione agli aggiornamenti emessi dalla stessa AGID;

- codice di condotta dell'Ente;

- GDPR sulla protezione dei dati laddove approvato;

- piano di formazione in materia di diritti e di liberta' delle persone e di protezione dei dati personali per i soggetti autorizzati al trattamento e per incaricati del back up;

- contratti/clausole contrattuali con i responsabili del trattamento;

- pareri del Responsabile protezione dati;

- verbali di vigilanza del responsabile protezione dati;

- circolari;

- informazioni fornite al pubblico e agli interessati;

- altra documentazione utile a comprovare la conformita' dei trattamenti al GDPR e alla normativa interna di adeguamento.

Contesto esterno: trattamenti affidati in outsourcing o effettuati da responsabili esterni

Contesto esterno: trattamenti affidati in outsourcing o effettuati da responsabili esterni

L'Elenco trattamenti affidati in outsourcing o comunque effettuati da responsabili esterni, e per formarne parte integrante sostanziale, consente di rilevare il rischio derivante dai trattamenti effettuate, nel contesto esterno alla struttura organizzativa del titolare.

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 31.000:2018, 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 sistematicamente nuove situazioni che potrebbero portare a rischi elevati per i diritti e le liberta' delle persone fisiche e non e' necessario realizzare una valutazione d'impatto sulla protezione dei dati nei casi (ad esempio operazioni di trattamento in un contesto specifico e per una finalita' specifica) che sono gia' stati studiati;

- la valutazione d'impatto va effettuata applicando le Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679;

- l'esito della valutazione va preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta il GDPR. In altre parole, una valutazione d'impatto sulla protezione dei dati e' un processo inteso a garantire e dimostrare la conformita'.

Va tenuto presente che l'inosservanza dei requisiti stabiliti per la valutazione d'impatto sulla protezione dei dati puo' portare a sanzioni pecuniarie imposte dall'autorita' di controllo competente. La mancata esecuzione di una valutazione d'impatto sulla protezione dei dati nei casi in cui il trattamento e' soggetto alla stessa (articolo 35, paragrafi 1, 3 e 4), l'esecuzione in maniera errata di detta valutazione (articolo 35, paragrafi 2 e da 7 a 9) oppure la mancata consultazione dell'autorita' di controllo laddove richiesto (articolo 36, paragrafo 3, lettera e)), possono comportare una sanzione amministrativa pecuniaria pari a un importo massimo di 10 milioni di EUR oppure, nel caso di un'impresa, pari a fino al 2% del fatturato annuo globale dell'anno precedente, a seconda di quale dei due importi sia quello superiore.

Determinazione di assoggettabilita' dei trattamenti a valutazione di impatto - DPIA

Preliminare per la valutazione di impatto e' la determinazione del titolare in ordine alla possibilita' che il trattamento possa determinare un rischio elevato per i diritti e le liberta' degli interessati.

La decisione in ordine alla possibilita' che il trattamento in epigrafe indicato possa produrre un rischio elevato sulla protezione dei dati delle persone fisiche e, quindi, sulla obbligatorieta' della DPIA viene adottata applicando i 3 casi indicati l'art. 35, paragrafo 3 del GDPR e i 9 CRITERI esplicativi contenuti nelle "Linee guida in materia

di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida").

Nell'applicare i suddetti CRITERI si deve tenere conto di quanto segue:

- la DPIA e' sempre obbligatoria, indipendentemente dalla presenza di uno o piu' criteri sopra menzionati, per tutti i trattamenti inclusi nell'elenco predisposto e pubblicato dall'Autorita' di controllo ai sensi dell'art. 35, paragrafo 4 GDPR;

- la DPIA e' sempre obbligatoria per i trattamenti inclusi nell'indice dei trattamenti dei dati sensibili e giudiziari ai sensi del Regolamento sul trattamento dei dati sensibili e giudiziari approvato dall'Ente conformemente allo schema tipo del Garante;

- 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 facente parte del sistema di organizzazione e di gestione del rischio di violazione dei dati personali (SOGDP), 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 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).

Per tali trattamenti:

- la determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (SCHEDE DPIA - FASE 1) dalle SCHEDE aventi funzione di RELAZIONE/REPORT;

- lo svolgimento della DPIA viene condotto secondo lo schema di flusso desunto dalle Linee guida in precedenza citate ed e' documentato e comprovato in atti (SCHEDE DPIA - FASE 2) dalle SCHEDE, aventi funzione di RELAZIONE/REPORT.

Il GDPR non definisce formalmente il concetto di valutazione d'impatto sulla protezione dei dati come tale, tuttavia il suo contenuto minimo e' specificato dall'articolo 35, paragrafo 7 GDPR, come segue:

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;

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 GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

In ordine ai diversi trattamenti, e sulla base determinazioni assunte in ordine alla possibilita' che il trattamento possa comportare un rischio elevato per i diritti e le liberta' degli interessati, le valutazioni di impatto documentate dalle SCHEDE (DPIA - FASE 2) vanno effettuate tenendo presente i ruoli stabiliti nelle Linee guida. In particolare:

a) il titolare del trattamento:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA;

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate;

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato;

- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.);

- 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 (31000:2018 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.

Lo scopo di un tale processo sarebbe quello di contribuire a stimolare la fiducia nei confronti dei trattamenti effettuati dal titolare del trattamento, nonche' di dimostrare la responsabilizzazione e la trasparenza. Costituisce una prassi particolarmente buona pubblicare una valutazione d'impatto sulla protezione dei dati nel caso in cui individui della popolazione siano influenzati dal trattamento interessato. Nello specifico, cio' potrebbe essere il caso in cui un'autorita' pubblica realizza una valutazione d'impatto sulla protezione dei dati.

La valutazione d'impatto sulla protezione dei dati pubblicata non deve necessariamente contenere l'intera valutazione, soprattutto qualora essa possa presentare informazioni specifiche relative ai rischi per la sicurezza per il titolare o un suo delegato del trattamento o divulgare segreti commerciali o informazioni commerciali sensibili. In queste circostanze, la versione pubblicata potrebbe consistere soltanto in una sintesi delle principali risultanze della valutazione d'impatto sulla protezione dei dati o addirittura soltanto in una dichiarazione nella quale si afferma che la valutazione d'impatto sulla protezione dei dati e' stata condotta.

Inoltre, laddove una valutazione d'impatto sulla protezione dei dati riveli la presenza di rischi residui elevati, il titolare o un suo delegato del trattamento sara' tenuto a richiedere la consultazione preventiva dell'autorita' di controllo in relazione al trattamento (articolo 36, paragrafo 1 GDPR). In tale contesto, la valutazione d'impatto sulla protezione dei dati deve essere fornita completa (articolo 36, paragrafo 3, lettera e GDPR).

Rischi residui e consultazione Autorita' di controllo

E' nei casi in cui il titolare del trattamento non riesca a trattare in maniera sufficiente i rischi individuati (ossia i rischi residui rimangono elevati) che questi deve consultare l'autorita' di controllo.

Un esempio di un rischio residuo elevato inaccettabile include casi in cui gli interessati possano subire conseguenze significative, o addirittura irreversibili, che non possono superare (ad esempio: accesso illegittimo a dati che comportano una minaccia per la vita degli interessati, un loro licenziamento, un rischio finanziario) e/o quando appare evidente che il rischio si verifichera' (ad esempio: poiche' non si e' in grado di ridurre il numero di persone che accedono ai dati a causa delle loro modalita' di condivisione, utilizzo o distribuzione o quando non si puo' porre rimedio a una vulnerabilita' ben nota).

Ogni qualvolta il titolare del trattamento non e' in grado di trovare misure sufficienti per ridurre i rischi a un livello accettabile (ossia i rischi residui restano comunque elevati) e' necessario consultare l'autorita' di controllo.

Inoltre, il titolare trattamento dovra' consultare l'autorita' di vigilanza qualora il diritto dello Stato membro in questione prescriva che il titolare del trattamento consultino l'autorita' di controllo e/o ne ottengano l'autorizzazione preliminare, in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanita' pubblica (articolo 36, paragrafo 5).

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 che:

- 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;

- o coinvolga le parti interessate appropriate e definisca chiaramente le loro responsabilita' (titolare del trattamento, responsabile della protezione dei dati, interessati o loro rappresentanti, imprese, servizi tecnici, responsabili del trattamento, responsabile della sicurezza dei sistemi d'informazione, ecc.);

- fornire la relazione relativa alla valutazione d'impatto sulla protezione dei dati all'autorita' di controllo, laddove gli venga richiesto di procedere in tal senso;

- consultare l'autorita' di controllo, qualora il titolare o un suo delegato del trattamento non sia riuscito a determinare misure sufficienti per attenuare i rischi elevati;

- riesaminare periodicamente la valutazione d'impatto sulla protezione dei dati e il trattamento che essa valuta, almeno quando si registra una variazione del rischio posto dal trattamento;

- documentare le decisioni prese.

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 ad 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.

Misure di sicurezza logistiche/fisiche

Sicurezza di aree e locali

L'identificazione delle misure di sicurezza logistiche/fisiche deve tenere conto almeno dei sotto indicati elementi di rischio, indicati a titolo esemplificativo e non esaustivo:

a) Collocazione

- Zona sismica

- Corsi d'acqua nelle vicinanze con rischio esondazione

- Aziende vicine con lavorazioni pericolose

- Installazioni vicine pericolose (aeroporti, depositi carburanti...)

- Area degradata

b) Vicinanza servizi

- Carabinieri o altre forze di polizia e vigilanza

- Ospedali o altri presidi

- Vigili del fuoco

c) Misure presenti anti intrusione

- Antifurto

- Vigilanza

- Videosorveglianza

- Controllo accessi

- Recinzioni

- Cancelli

d) Misure presenti anti incendio

- Estintori

- Idranti

- Rilevatori

e) Misure presenti per la regolarita' degli impianti

- Elettrico

- Climatizzazione

- Riscaldamento

f) Misure presenti per la continuita' elettrica

- UPS

- Generatori

g) 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

- Allarmi

- Connessione con le forze dell'ordine

- Connessione con servizi di vigilanza

- Videosorveglianza

- Porta normale

- Porta blindata

- Serratura di sicurezza

- Finestre con grate

- Finestre senza grate

b) antincendio

- Sensori

- Allarmi

- Estintori/Impianto antincendio

- Impianti a norma

- Porta taglia fuoco

- Porta antincendio per fuga

- Utilizzo materiale ignifugo

c) Sicurezza ambientale

- Piano di emergenza per la gestione dei rischi individuati

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

- Posizionamento ordinato delle apparecchiature nei rack

- Spazio intorno ai rack adeguato per la movimentazione e manutenzione delle apparecchiature

g) Sistema di custodia archivi cartacei

- Armadi blindati

- Armadi ignifughi con serratura

- Armadi ignifughi senza serratura

- Altri armadi con serratura

- Altri armadi senza serratura

- Classificatori/cassetti con serratura

- Classificatori/cassetti senza serratura

- Cassaforte

- Scaffalature

La MAPPA delle misure delle misure di sicurezza logistiche/fisiche applicate i diversi trattamenti, facente parte del sistema di organizzazione e di gestione del rischio di violazione dei dati personali (SOGDP), documenta e comprova l'osservanza del GDPR.

Misure di sicurezza informatiche/logiche

Al fine di indicare alle pubbliche amministrazioni le misure minime per la sicurezza ICT che debbono essere adottate per contrastare le minacce piu' comuni e frequenti cui sono soggetti i loro sistemi informativi, ed in adeguamento della Direttiva 1 agosto 2015 del Presidente del Consiglio dei Ministri che emana disposizioni finalizzate a consolidare lo stato della sicurezza informatica nazionale, AgID ha provveduto ad emanare l'elenco ufficiale delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni".

Con l'avvenuta pubblicazione in Gazzetta Ufficiale (Serie Generale n.103 del 5-5-2017) della Circolare 18 aprile 2017, n. 2/2017, recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1 agosto 2015)", le Misure minime sono ora divenute di obbligatoria adozione per tutte le Amministrazioni.

L'adeguamento dell'Ente alle Misure minime e' stato completato dall'Ente, 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.

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.

Per l'identificazione delle 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 delle misure di sicurezza logistiche/fisiche applicate i diversi trattamenti inclusi i criteri e modalita' di salvataggio e di ripristino della disponibilita' dei dati, facente parte del sistema di organizzazione e di gestione del rischio di violazione dei dati personali (SOGDP), 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

d) al controllo degli accessi degli archivi/banche dati";

- esercizio diritti: misure organizzative 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";

- formazione: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'unione o degli stati membri;

- gestione dati: distruzione documenti non necessari;

- gestione dati: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del garante";

- gestione dati: separazione documenti e dati;

- gestione dati: utilizzazione documenti;

- informazione: informazione continua e aggiornamento costante su procedure operative e istruzioni;

- prescrizioni: nell'attivita' di videosorveglianza prescrizione del rispetto di tutte le misure e gli accorgimenti prescritti autorita' Garante come esito di una verifica preliminare attivata d'ufficio o a seguito di un interpello";

- trattamenti senza l'uso di strumenti elettronici: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative;

- work flow: in applicazione dei principi della norma uni iso 31000:2018, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti";

- work flow: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento.

La MAPPA delle misure di sicurezza organizzative, applicate i diversi trattamenti ,facente parte del sistema di organizzazione e di gestione del rischio di violazione dei dati personali (SOGDP), documenta e comprova l'osservanza del GDPR.

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";

- definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi";

- definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000:2018 e del GDPR".

La MAPPA delle misure di sicurezza procedurali, applicate ai diversi trattamenti facente parte del sistema di organizzazione e di gestione del rischio di violazione dei dati personali (SOGDP), documenta e comprova l'osservanza del GDPR.

Piano formativo

La formazione in materia di trattamento e di protezione dei dati personali costituisce una misura di sicurezza e, in quanto tale, e' da intendersi obbligatoria.
Annualmente va approvato il piano formativo in materia di trattamento e di protezione dei dati personali.

Il piano formativo deve essere definito sulla base dei seguenti CRITERI:

a) Formazione di base di primo livello di natura giuridica avente ad oggetto il trattamento dei dati personali, comprese tutte le tecniche da applicare al medesimo trattamento nonche' la protezione da assicurare ai diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali

b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000:2018 e del RGDPR;

c) Identificazione di procedure idonee per selezionare e formare i soggetti del sistema di protezione, come identificati nel presente PPD, da formare adeguatamente.

Codici di condotta
Per i codici di condotta si rinvia ai codici approvati dal Garante , compresi i codici approvati ai sensi degli artt. 40, par. 5, 57, par. 1, lett. m) e 58, par. 3, lett. d) del Regolamento, e si richiamano contestualmente il DPR n. 62/2013 nonche' al codice di comportamento approvato dal titolare ad integrazione del citato DPR n. 62/2013.

Certificazione
Si rinvia alla certificazione eventualmente acquisita per formare parte integrante e sostanziale del presente PPD.

Notifica di una violazione dei dati personali all'Autorita' di controllo
Violazione dei dati personali
L'amministrazione si dota di un Registro per tracciare documentalmente violazioni di sicurezza.

Il contenuto e le modalita' di aggiornamento del Registro sono definite nell'ambito di una apposita procedura operativa facente parte del sistema di organizzazione e di gestione del rischio di violazione dei dati personali (SOGDP).

Per le notifiche all'Autorita' di controllo, il presente PPD rinvia alla definizione e attuazione di adeguate misure organizzative e procedurali, ferma restando la disciplina del GDPR.

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.

ALLEGATI

01 - STRUTTURA ORGANIZZATIVA ED ELENCO DEI SOGGETTI INTERNI ED ESTERNI

02 - SCHEDE DI RICOGNIZIONE TRATTAMENTI ED INDICE MAPPA TRATTAMENTI

03 - SCHEDE DI VALUTAZIONE DI IMPATTO (DPIA) TRATTAMENTI A RISCHIO ELEVATO

04 - SCHEDE DI SINTESI DPIA

05 - MISURE DI PROTEZIONE DATI

06 - MAPPA RISCHI E MOTIVAZIONI DI STIMA

07 - MAPPA DEI LUOGHI

08 - MAPPA HARDWARE SOFTWARE CON INDICAZIONE DI ARCHIVI E BANCHE DATI ELETTRONICHE

09 - MODELLI ATTI DI DELEGA ED INCARICO AL TRATTAMENTO DATI

10 - CORSI DI FORMAZIONE