COMUNE DI ANDORA

PROVINCIA DI SAVONA

Regolamento sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Adeguamento al Regolamento (UE) 2016/697 e al Decreto legislativo 10 agosto 2018 n. 101.

ELENCO DELIBERE

1 – C.C. n. xx del xx.xx.2018: "Approvazione regolamento sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali. Adeguamento al Regolamento (UE) 2016/679 e al Decreto legislativo 10 agosto 2018 n. 101"

SOMMARIO

INTRODUZIONE

Il 27 aprile 2016 è stato approvato il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, con abrogazione della direttiva 95/46/CE (Regolamento generale sulla protezione dei dati).

Il nuovo regolamento UE, che si applica negli Stati membri a decorrere dal 25 maggio 2018, si fonda sulla affermazione che la protezione delle persone fisiche, con riguardo al trattamento dei dati di carattere personale, è un diritto fondamentale come risulta anche dalla circostanza che l'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

Per rafforzare la protezione, il Regolamento UE, introduce numerose e rilevanti novità partendo da un approccio, fondato sul principio di cautela, basato sul rischio del trattamento e su misure di accountability di titolari e responsabili (come la valutazione di impatto, il registro dei trattamenti, le misure di sicurezza, la nomina di un Responsabile Della Protezione-Data Protection Officer).

Come ha evidenziato il Garante nella guida all'applicazione del Regolamento, la nuova disciplina europea pone con forza l'accento sulla "responsabilizzazione" ossia, sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento. Tra i criteri che i titolari e i responsabili sono tenuti ad utilizzare nella gestione degli obblighi vi sono:

- il criterio del "data protection by default and by design", ossia la necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati;
- il criterio del rischio inerente al trattamento, da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati, impatti che devono essere analizzati attraverso un apposito processo di valutazione tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il Titolare ritiene di dover adottare per mitigare tali rischi.

Ne consegue che l'intervento delle autorità di controllo, nel nuovo impianto gestionale, è destinato a svolgersi principalmente ex post, ossia a collocarsi successivamente alle determinazioni assunte autonomamente dal Titolare; ciò spiega l'abolizione, a partire dal 25 maggio 2018, di alcuni istituti previsti dalla direttiva del 1995 e dal Codice italiano, come la notifica preventiva dei trattamenti all'autorità di controllo e il cosiddetto prior checking (o verifica preliminare), sostituiti da obblighi di tenuta di un registro dei trattamenti da parte del Titolare/Responsabile e, appunto, di effettuazione di valutazioni di impatto in piena autonomia.

Lo stato italiano in attuazione della delega legislativa di cui alla Legge 25 ottobre 2017 n. 163 ha approvato il 10 agosto 2018 il decreto legislativo 101 ad oggetto "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del

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, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati." In GU n. 205 del 4.9.2018 in vigore dal 19.9.2018.

Il Comune di Andora, Titolare del trattamento, intende adeguare e conformare la propria normativa regolamentare alle novellate disposizioni in materia di protezione dei dati personali ed ha già provveduto entro il 25 maggio 2018 alla individuazione del Responsabile della Protezione dei Dati.

CAPO I – DISPOSIZIONI GENERALI

Art. 1 – Definizioni

Il presente regolamento si avvale delle seguenti definizioni:

- "Codice": il D.Lgs. n. 196/2003 così come da ultimo modificato dal Decreto legislativo 101 del 10 agosto 2018;

- "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, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (GDPR generale sulla protezione dei dati);

- "Regolamento per la protezione dei dati sensibili e giudiziari": il Regolamento interno, approvato con Delibera di Consiglio Comunale n. 22 del 15 maggio 2006 n. 22 in conformità 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;

- "Regolamento sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali adottato in attuazione del Regolamento UE 2016/679 e al Decreto legislativo 10 agosto 2018 n. 101" il presente Regolamento;

- "Titolare del trattamento": la persona fisica o giuridica, che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; il Titolare del trattamento è il Comune di Andora che adotta il presente regolamento,

- "Responsabili del trattamento" i soggetti (dirigenti/P.O). che esercitano i poteri espressamente delegati dal Titolare o che sono nominati dal Titolare per esercitare tali poteri;

- "Incaricati": le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile;

- "Responsabile della Protezione dei Dati RPD/DPO" il soggetto che fornisce consulenza al Titolare del trattamento in merito agli obblighi vigenti relativi alla protezione dei dati, verifica l'attuazione e l'applicazione della normativa vigente in materia, funge da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento dei dati, tra cui la consultazione preventiva;

- "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;

"Dati sensibili": i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso,

filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

- "Dati giudiziari": i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o), e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

- "Interessato": la persona fisica, cui si riferiscono i dati personali;

- "Comunicazione" dare conoscenza con qualsiasi forma di dati personali a uno o più soggetti determinati diversi dall' interessato e dalle persone autorizzate al trattamento;

- "Diffusione" dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante consultazione;

- "Garante": l'autorità di cui all'articolo 153 D.Lgs. 196/2003, istituita dalla legge 31 dicembre 1996, n. 675 è autorità di controllo e consulenza in materia di protezione dei dati.

Art. 2 – Quadro normativo di riferimento

Il presente Regolamento tiene conto dei seguenti documenti:

- Codice in materia di dati personali (D.Lgs. n. 196/2003) così come da ultimo modificato ed integrato dal Decreto legislativo 101 del 10 agosto 2018;

- 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, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;

- 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, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;

Alla emanazione delle regole deontologiche da parte del Garante, nonché dei Decreti attutativi previsti dal D.Lgs. 101/2018 verranno adottate, se del caso, integrazioni del presente Regolamento.

Art. 3 – Oggetto

Il presente Regolamento ha per oggetto la protezione dei diritti e delle libertà delle persone fisiche in ordine al trattamento dei dati personali effettuato dal Titolare, nel rispetto di quanto previsto dal GDPR.

Il presente Regolamento integra il Regolamento sui dati sensibili e giudiziari, approvato con deliberazione C.C. n. 22 del 15 maggio 2006 e conferma le schede/tabelle allegate al Regolamento medesimo, che identificano i tipi di dati sensibili e giudiziari per cui è consentito il relativo trattamento, nonché le operazioni eseguibili in riferimento alle specifiche finalità di rilevante interesse pubblico perseguite nei singoli casi ed espressamente elencate dalla legge, le quali continuano ad applicarsi e vengono allegate al presente Regolamento per farne parte integrante e sostanziale.

Art. 4 – Finalità

Il Titolare garantisce che il trattamento dei dati, a tutela delle persone fisiche, si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o della loro residenza.

Il Titolare, nell'ambito delle sue funzioni, gestisce gli archivi e le banche dati rispettando i diritti, le libertà fondamentali e la dignità delle persone, con particolare riferimento alla riservatezza e all'identità personale.

Ai fini della tutela dei diritti e delle libertà delle persone fisiche in ordine al trattamento dei dati personali, tutti i processi, inclusi i procedimenti amministrativi di competenza del Titolare, vanno gestiti conformemente alle disposizioni del Codice, del GDPR, e del presente Regolamento.

CAPO II – PRINCIPI

Art. 5 – Principi e responsabilizzazione

Vengono integralmente recepiti, nell'ordinamento interno del Titolare, i principi del GDPR, per effetto dei quali dati i personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza");

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

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati base del principio di "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 finalità per le quali sono trattati base del principio di "esattezza";

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato in base al principio di "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 in base ai principi di "integrità e riservatezza";

g) configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità possano essere perseguite mediante dati anonimi o con l'uso di opportune modalità che permettono di identificare l'interessato solo un caso di necessità ("principio di necessità").

Il Titolare è competente per il rispetto dei principi sopra declinati, ed è in grado di comprovarlo in base al principio di "responsabilizzazione".

Art. 6 – Liceità del trattamento

Vengono integralmente recepiti, nell'ordinamento interno del Titolare, le disposizioni del GDPR in odine alla liceità del trattamento e, per l'effetto, il trattamento è lecito 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 più specifiche finalità;

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

c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare del trattamento;

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

e) il trattamento è 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 libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore;

f) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico "rilevante" connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento. Si intende rilevante l' interesse pubblico relativo a trattamenti effettuati nelle seguenti materie:

1) accesso a documenti amministrativi e accesso pubblico;

2) tenuta atti e registri stato civile, anagrafe, liste elettorali, rilascio di documenti di riconoscimento o di viaggio o cambiamento delle generalità;

3) tenuta dei registri pubblici relativi a beni immobili e mobili;

4) tenuta dell'anagrafe nazionale degli abilitati alla guida e dell' archivio nazionale dei veicoli;

5) cittadinanza, immigrazione, asilo, condizione dello straniero e del profugo, stato di rifugiato;

6) elettorato attivo e passivo ed esercizio dei diritto politici, protezione diplomatica e consolare, nonché documentazione delle attività istituzionali di organi pubblici, con particolare riguardo alla redazione di verbali e resoconti della attività di assemblee rappresentative, commissioni ed altri organi collegiali o assembleari;

7) esercizio del mandato degli organi rappresentativi, ivi compresa la loro sospensione o il loro scioglimento, nonché l'accertamento delle cause di ineleggibilità, incompatibilità, decadenza, ovvero di rimozione o sospensione da cariche pubbliche;

8) svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso ai documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalità direttamente connesse all' espletamento del mandato elettivo;

9) attività dei soggetti pubblici dirette alla applicazione, anche tramite i loro concessionari, delle disposizioni in materia tributaria e doganale;

10) attività di controllo ed ispettive;

11) concessione, liquidazione e revoca di benefici economici, agevolazioni. elargizioni, altri emolumenti ed abilitazioni;

12) conferimento di onorificenze e ricompense, riconoscimento della personalità giuridica di associazioni, fondazioni ed enti, anche di culto, accertamento dei requisiti di onorabilità e di professionalità per le nomine, per i profili di competenza del soggetto pubblico, ed uffici anche di culto e cariche direttive di persone giuridiche, imprese ed istituzioni scolastiche non statali, nonché rilascio e revoca di autorizzazioni ed abilitazioni, concessione di patrocini, patronati e premi di rappresentanza, adesione a comitati d'onore e ammissione a cerimonie ed incontri istituzionali;

13) rapporti tra soggetti pubblici ed enti del terzo settore;

14) obiezione di coscienza;

15) attività sanzionatorie e di tutela in sede amministrativa e giudiziaria;

16) rapporti istituzionali con enti di culto, confessioni religiose e comunità religiose;

17) attività socio-assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci;

18) attività amministrative e certificatorie correlate a quelle di diagnosi, assistenza o terapia sanitaria o sociale, ivi incluse quelle correlate a trapianti di organi e di tessuti, nonché alla trasfusioni di sangue umano;

19) compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita ed incolumità fisica;

20) programmazione, gestione, controllo e valutazione dell' assistenza sanitaria, ivi incluse l' instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale;

21) vigilanza sulle sperimentazioni, farmacovigilanza, autorizzazione all' immissione in commercio e all' importazione di medicinali e di altri prodotti di rilevanza sanitaria;

22) tutela sociale della maternità e interruzione volontaria della gravidanza, dipendenze, assistenza, integrazione sociale e diritti dei disabili,

23) istruzione e formazione in ambito scolastico, professionale, superiore o universitario;

24) trattamenti effettuati ai fini di archiviazione, nel pubblico interesse o di ricerca storica, concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di stato negli archivi storici degli enti pubblici, o in archivi privati dichiarati di interesse storico particolarmente importante, per fini di ricerca scientifica, nonché per fini statistici da parte di soggetti che fanno parte del sistema statistico nazionale (Sistan);

25) instaurazione, gestione ed estinzione di rapporti di lavoro di qualunque tipo, anche non retribuito ed onorario, e di altre forme di impego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunità nell' ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza e salute della popolazione, accertamento della responsabilità civile, disciplinare e contabile, attività ispettiva.

Art. 7 – Condizioni per il consenso

Nei casi in cui il trattamento dei dati personali, per una o più specifiche finalità, è subordinato al consenso dell'interessato, si applica la disciplina del GDPR la quale prevede che:

- qualora il trattamento sia basato sul consenso, il Titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali;

- il consenso già prestato ai sensi della normativa e del regolamento previgenti rimane valido per le attività di trattamento già autorizzate e per quelle future che non contrastino con il presente regolamento;

- se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è 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 è vincolante;

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

- nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, 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.

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

- il consenso dei minori è valido a partire dai 16 anni, ovvero di 14 anni per l' accesso ai servizi della società dell' informazione; prima di del limite età occorre raccogliere il consenso dei genitori o di chi ne fa le veci;

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

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

- nessuna parte di una tale dichiarazione, che costituisca una violazione del GDPR e del presente Regolamento, è vincolante.

In caso di impossibilità fisica, incapacità di agire o incapacità di intendere e di volere dell'interessato, emergenza sanitaria o di igiene pubblica, rischio grave e imminente per la salute dell'interessato, il consenso può intervenire senza ritardo, anche successivamente alla prestazione, da parte di chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente.

Qualora il trattamento sia basato sul consenso, il consenso deve essere reso, da parte dell'interessato, attraverso la compilazione di apposita modulistica, predisposta dal Titolare, previa consegna e presa d'atto dell'informativa.

Non è ammesso il consenso tacito o presunto ovvero l'utilizzo di caselle pre-spuntate su un modulo.

Il Titolare adotta misure organizzative adeguate a facilitare l'espressione del consenso da parte dell'interessato.

La manifestazione del consenso, ad opera dell'interessato, va resa al momento del primo accesso alle prestazioni, ed è valido ed efficace fino alla revoca della stessa o, per i minorenni, fino al compimento del diciottesimo anno di età.

Il consenso viene registrato nel registro delle attività di trattamento.

Art. 8 – Informativa

Il Titolare, al momento della raccolta dei dati personali, è tenuto a fornire all'interessato, anche avvalendosi del personale incaricato, apposita informativa secondo le modalità previste dal GDPR e dall'art 13 Codice, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.

L'informativa è 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.

L'informativa è fornita, mediante idonei strumenti:

• attraverso appositi moduli (come da modello allegato al presente regolamento) da consegnare agli interessati, per l'accesso alle prestazioni gestite in forma cartacea. Nel modulo sono indicati i soggetti a cui l'utente può rivolgersi per ottenere maggiori informazioni ed esercitare i propri diritti, anche al fine di consultare l'elenco aggiornato dei responsabili;

• apposita avvertenza inserita nei contratti ovvero nelle lettere di affidamento di incarichi del personale dipendente, dei soggetti con i quali vengono instaurati rapporti di collaborazione o libero-professionali, dei tirocinanti, dei volontari, degli stagisti ed altri soggetti che entrano in rapporto con il Titolare;

• apposita avvertenza inserita in sede di pubblicazione dei bandi, avvisi, lettere d'invito, con l'indicazione dell'incaricato del trattamento dei dati relativi alle procedure;

• attraverso la pubblicazione di avvisi agevolmente visibili per l'accesso alle prestazioni tramite portali elettronici, nonché mediante esposizione sul sito internet del Titolare della Privacy policy;

L'informativa da fornire agli interessati può essere fornita anche in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto.

Se presentate elettronicamente, le icone sono leggibili da dispositivo automatico.

L'informativa contiene il seguente contenuto minimo:

• l'identità e i dati di contatto del Titolare e, ove presente, del suo rappresentante;

• i dati di contatto del RPD;

• le finalità del trattamento;

• i destinatari dei dati;

• la base giuridica del trattamento;

• l' interesse legittimo del Titolare se quest'ultimo costituisce la base giuridica del trattamento;

• se il Titolare trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti;

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

• il diritto dell'interessato di chiedere al Titolare l'accesso, la rettifica, la cancellazione dei dati, la limitazione del trattamento che lo riguarda, il diritto di opporsi al trattamento e il diritto alla portabilità dei dati;

• il diritto di presentare un reclamo all'autorità di controllo;

• l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e le informazioni significative sulla logica utilizzata nonché l'importanza e le conseguenze di tale trattamento per l'interessato.

Nel caso di dati personali non raccolti direttamente presso l'interessato:

a) il Titolare deve informare l'interessato in merito a:

- le categorie di dati personali trattati;

- la fonte da cui hanno origine i dati personali e l'eventualità che i dati provengano da fonti accessibili al pubblico;

b) l'informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure dal momento della comunicazione (e non della registrazione) dei dati a terzi o all'interessato.

Per i trattamenti dei dati connessi alla gestione del rapporto di lavoro con il personale dipendente del Titolare è predisposta apposita informativa per personale dipendente.

Apposite informative devono essere inserite nei seguenti documenti:

- nei bandi e nella documentazione di affidamento dei contratti pubblici, nei contratti, accordi o convenzioni, nei bandi di concorso pubblico, nelle segnalazioni di disservizio e, più in generale, in ogni altro documento contenente dati personali.

Nel fornire l'informativa, il Titolare fa espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati sensibili e giudiziari.

Art. 9 – Sensibilizzazione e formazione

Ai fini della corretta e puntuale applicazione della disciplina relativa ai principi, alla liceità del trattamento, al consenso, all'informativa e, più in generale, alla protezione dei dati personali, il Titolare sostiene e promuove, all'interno della propria struttura organizzativa, ogni strumento di sensibilizzazione che possa consolidare la consapevolezza del valore della riservatezza dei dati, e migliorare la qualità del servizio.

A tale riguardo, il presente regolamento riconosce che uno degli strumenti essenziali di sensibilizzazione è l'attività formativa del personale del Titolare e l'attività informativa diretta a tutti coloro che hanno rapporti con il Titolare.

Per garantire la conoscenza capillare delle disposizioni del presente Regolamento, al momento dell'ingresso in servizio è data a ogni dipendente una specifica comunicazione, con apposita clausola inserita nel contratto di lavoro, contenente tutti i principi fondamentali della materia, esposti in maniera semplice, chiara e puntuale, con i riferimenti per l'acquisizione del presente Regolamento, pubblicato sul sito del Titolare.

Il Titolare organizza, nell'ambito della formazione continua e obbligatoria del personale, specifici interventi di formazione e di aggiornamento, anche integrati con gli interventi di formazione anticorruzione, in materia di protezione dei dati personali, finalizzati alla conoscenza delle norme, alla prevenzione di fenomeni di abuso e illegalità nell'attuazione della normativa, all'adozione di idonei modelli di comportamento e procedure di trattamento, alla conoscenza delle misure di sicurezza per il trattamento e la conservazione dei dati, dei rischi individuati e dei modi per prevenire danni agli interessati.

La formazione in materia di prevenzione dei rischi di violazione dei dati personali viene integrata e coordinata, a cura del RPC, con la formazione in materia di prevenzione della corruzione e della illegalità nonché con la formazione in tema di trasparenza e di accesso, con particolare riguardo ai rapporti tra protezione dei dati personali, trasparenza accesso ai documenti amministrativi e accesso civico, semplice e generalizzato, nei diversi ambiti in cui opera il Titolare.

La partecipazione dei dipendenti agli interventi formativi viene considerata quale elemento di misurazione e valutazione della performance organizzativa ed individuale.

La formazione di base di Dirigenti e PO sul GDPR è stata effettuata alla entrata in vigore del Regolamento (EU) 697/2016.

CAPO III – IL TRATTAMENTO DEI DATI PERSONALI

Art. 10 – Trattamento dei dati personali, ricognizione dei trattamenti e indice dei trattamenti

Il Titolare tratta i dati personali per lo svolgimento delle proprie finalità istituzionali, come identificate da disposizioni di legge, statutarie e regolamentari, e nei limiti imposti dal Codice, dal GDPR e dalle Linee Guida e dai i provvedimenti del Garante.

Il Titolare effettua i trattamenti di dati personali, previsti da disposizioni legislative e regolamentari riguardanti, a titolo esemplificativo e non esaustivo:

- la gestione del personale dipendente, ivi comprese le procedure di assunzione;
- la gestione dei soggetti che intrattengono rapporti giuridici con il Titolare, diversi dal rapporto di lavoro dipendente, e che operano a qualsiasi titolo all'interno della struttura organizzativa del Titolare, ivi compresi gli stagisti, tirocinanti e i volontari;
- la gestione dei rapporti con i consulenti, i libero-professionisti, i fornitori per l'approvvigionamento di beni e di servizi nonché con le imprese per l'esecuzione lavori, opere e di interventi di manutenzione;
- la gestione dei rapporti con i soggetti accreditati o convenzionati per i servizi socio-assistenziali;
- la gestione dei rapporti con la Procura della Repubblica e gli altri soggetti pubblici competenti, per le attività ispettive di vigilanza, di controllo e di accertamento delle infrazioni alle leggi e regolamenti.

Il trattamento dei dati personali è esercitabile, all'interno della struttura organizzativa del Titolare, solo da parte dei soggetti appositamente autorizzati:

- Titolare
- Responsabili, individuati nei Dirigenti/PO., in qualità di soggetti che esercitano i poteri delegati dal Titolare o in qualità di soggetti nominati dal Titolare per l'esercizio di tali poteri
- dipendenti, in qualità di incaricati del trattamento

Non è consentito il trattamento da parte di persone non autorizzate.

Ai fini del trattamento, il Titolare provvede, in collaborazione con i Resaponsabili., alla integrale ricognizione e all'aggiornamento di tutti i trattamenti di

dati personali effettuati nell'ambito dei processi e procedimenti del Titolare medesimo, funzionali alla formazione dell'indice dei trattamenti.

È compito dei Resaponsabili dei dati effettuare e documentare l'aggiornamento periodico della ricognizione dei trattamenti e del relativo indice, e la valutazione del rispetto dei principi di cui all'art. 5 del presente Regolamento con riferimento a tutti trattamenti inclusi nell'indice.

Il Titolare, i responsabili e gli incaricati si attengono alle modalità di trattamento indicate nel Codice, nel GDPR, nonché nelle regole deontologiche definite dal Garante per la protezione dei dati personali e nei Decreti attuativi previsti nel Decreto legislativo 101 del 2018.

Art. 11 – Tipologie di dati trattati

Nell'ambito dei trattamenti inclusi nell'indice dei trattamenti, il Titolare, nell'esercizio delle sue funzioni istituzionali, tratta in modo anche automatizzato, totalmente o parzialmente, le seguenti tipologie di dati:

- dati comuni identificativi
- dati sensibili
- dati giudiziari.

Art. 12 – Trattamento dei dati relativi a condanne penali e reati

Il Titolare conforma il trattamento dei dati giudiziari secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato, ed è consentito solo se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, che prevedano garanzie appropriate per i diritti e le libertà degli interessati.

Sono inoltre autorizzati i trattamenti individuati con apposito Decreto del Ministero di Giustizia, (così come previsto dal D. Lgs. 101/2018), riguardanti condanne penali, reati o misure di sicurezza per :

a) l' adempimento di obblighi e l' esercizio di diritti in materia di lavoro nei limite stabiliti da leggi, regolamenti e contratti collettivi;

b) l'adempimento di obblighi in materia di mediazione per la conciliazione di controversie civili e commerciali;

c) la verifica dei requisiti di onorabilità, requisiti soggettivi e presupposti interdettivi;

d) l' accertamento della responsabilità in relazione a sinistri, nonché la prevenzione di frodi;

e) l' accertamento l' esercizio e la difesa di diritto in sede giudiziaria;

f) l'esercizio dei diritti di accesso a dati e documenti nei limiti di quanto previsto dalle leggi e dai regolamenti in materia;

g) l'esecuzione di investigazioni o ricerche o raccolta di informazioni presso terzi ai sensi dell' art. 134 del tersto unico delle leggi di pubblica sicurezza;

h) l'adempimento di obblighi in materia di comunicazioni e informazioni antimafia o per la produzione della documentazione prescritta per partecipare a gare d'appalto;

i) l'accertamento dei requisiti di idoneità morale di coloro che intendono partecipare a gare di appalto, in adempimento della normativa in materia di appalti;

j) l'attuazione della disciplina del rating di legalità delle imprese;

k) l'adempimento degli obblighi previsti dalla normativa antiriciclaggio.

Il Decreto del Ministero della Giustizia autorizza il trattamento dei dati effettuato in attuazione dei protocolli di intesa per la prevenzione ed il contrasto della criminalità organizzata di concerto con il Ministero dell' Interno e le Prefetture UTG.

Il Titolare sensibilizza, forma e aggiorna i dipendenti in ordine al trattamento dei dati sensibili e giudiziari.

I dati personali trattati in violazione della disciplina in materia di trattamento non possono essere utilizzati salvo quanto previsto dall' art 160 bis del Codice relativamente all' uso nei procedimenti giudiziari.

Art. 13 – Trattamento dei dati sensibili relativi alla salute

Il Titolare si conforma alle misure di garanzia disposte dal Garante con cadenza biennale in materia di trattamento dei dati personali sensibili relativi allo stato di salute, ai dati genetici e biometrici che non possono essere diffusi.

Le misure di garanzia da adottare a cura del Garante riguarderanno i contrassegni sui veicoli e gli accessi alle zone a traffico limitato, le ulteriori misure di sicurezza, ivi comprese le tecniche di cifratura e pseudonimizzazione.

I dati idonei a rivelare lo stato di salute sono trattati da soggetti adeguatamente formati e sono conservati separatamente da ogni altro dato personale trattato per finalità che non richiedono il loro utilizzo.

Art. 14 – Trattamento dei dati del personale

Il Titolare tratta i dati, anche di natura sensibile o giudiziaria, dei propri dipendenti per le finalità, considerate di rilevante interesse pubblico, di instaurazione e di gestione di rapporti di lavoro di qualunque tipo.

Tra tali trattamenti sono compresi quelli effettuati al fine di accertare il possesso di particolari requisiti previsti per l'accesso a specifici impieghi, la sussistenza dei presupposti per la sospensione o la cessazione dall'impiego o dal servizio, di adempiere agli obblighi connessi alla definizione dello stato giuridico od economico del personale, nonché ai relativi obblighi retributivi, fiscali e contabili, relativamente al personale in servizio o in quiescenza.

Secondo la normativa vigente, il Titolare adotta le massime cautele nel trattamento di informazioni personali del proprio personale dipendente che siano idonee a rivelare lo stato di salute, le abitudini sessuali, le convinzioni politiche, sindacali, religiose filosofiche o d'altro genere e l'origine razziale ed etnica.

Il trattamento dei dati sensibili del dipendente, da parte del datore di lavoro, deve avvenire secondo i principi di necessità e di indispensabilità che impongono di ridurre al minimo l'utilizzo dei dati personali, e quando non si possa prescindere dall'utilizzo dei dati giudiziari e sensibili, di trattare solo le informazioni che si rivelino indispensabili per la gestione del rapporto di lavoro.

Il trattamento dei dati presenti nei curricula spontaneamente trasmessi non necessita di consenso.

La pubblicazione delle graduatorie di selezione del personale o relative alla concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, deve essere effettuata dopo un'attenta verifica che le indicazioni contenute non comportino la divulgazione di dati idonei a rivelare lo stato di salute, utilizzando diciture generiche o codici numerici. Non sono infatti ostensibili, se non nei casi previsti dalla legge, le notizie concernenti la natura delle infermità e degli impedimenti personali o familiari che causino l'astensione del lavoro, nonché le componenti della valutazione o le notizie concernenti il rapporto di lavoro tra il personale dipendente e l'amministrazione, idonee a rivelare taluna delle informazioni di natura sensibile.

Il Titolare, nel trattamento dei dati sensibili relativi alla salute dei propri dipendenti, deve rispettare i principi di necessità e indispensabilità.

Il Titolare si conforma alle Linee Guida del Garante in materia di trattamento dei dati personali dei lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico.

Art. 15 – Rilevanza delle schede identificative delle tipologie di tipi di dati sensibili e giudiziari per cui è consentito il relativo trattamento

Le schede identificative delle tipologie di dati sensibili e giudiziari per cui è consentito il relativo trattamento da parte del Titolare, nonché le operazioni eseguibili in riferimento alle specifiche finalità di rilevante interesse pubblico, rappresentative dell'indice dei trattamenti, allegate al regolamento approvato con deliberazione CC. n. 22 del 15 maggio 2006 e che continuano ad applicarsi venendo allegate al presente Regolamento:

a) vanno consegnate, personalmente, agli incaricati a cui, in materia o competenza, si riferiscono;

b) costituiscono oggetto di formazione;

c) costituiscono oggetto di interventi di monitoraggio e di verifica con riguardo alla loro applicazione;

d) costituiscono parti essenziali del Registro dei trattamenti del Titolare e dei Responsabili.

Art. 16 – Registro delle attività di trattamento e delle categorie di trattamento

Il Titolare del trattamento istituisce un registro, in forma scritta digitale, delle attività di trattamento e delle categorie di trattamenti svolte sotto la propria responsabilità.

Il registro deve essere continuamente aggiornato e messo a disposizione delle autorità di controllo. Tale registro contiene le seguenti informazioni:

1 il nome e i dati di contatto del Titolare del trattamento, del Responsabile per la protezione dei dati, dei responsabili e degli incaricati;

2 le finalità del trattamento;

3 una descrizione delle categorie di interessati e delle categorie dei dati personali;

4 le categorie dei trattamenti effettuati;

5 la categorie di destinatari, a cui i dati personali sono o saranno comunicati;

6 l'indicazione delle cautele specifiche, a cui ciascun Responsabile deve attendere in modo che siano appropriate rispetto ai trattamenti verso cui dovrà rispondere;

7 un'eventuale possibilità di trasferimenti di dati all'estero;

8 una descrizione generale delle misure di sicurezza, generiche e specifiche, così come disciplinate dalla normativa vigente in tema di sicurezza dei dati personali;

9 indicazione dei termini ultimi previsti per la cancellazione delle diverse categorie di dati trattati.

Il registro per i punti 2-3-4 e 5 è costituito dagli allegati al presente regolamento

Il Responsabile di trattamento tiene registro di tutte le categorie di attività relative al trattamento svolte per conto di un Titolare del trattamento, contenente:

a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni Titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del Titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;

b) le categorie dei trattamenti effettuati per conto di ogni Titolare del trattamento;

c) ove applicabile, i trasferimenti di dati personali verso un Paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1 GDPR.

I registri dei Responsabili sono tenuti in forma scritta in formato elettronico.

Su richiesta, il Titolare del trattamento o il responsabile del trattamento, mettono il registro a disposizione del Garante.

CAPO IV – DIRITTI DEGLI INTERESSATI

Art. 17 – Pubblicità e diffusione di dati personali contenuti in atti e provvedimenti amministrativi

Il Titolare, in sede di pubblicazione e diffusione, tramite l'albo pretorio informatico e la rete civica, di dati personali contenuti in atti e provvedimenti amministrativi, assicura, mediante l'implementazione delle necessarie misure tecniche ed organizzative, il rispetto dei seguenti principi:

a) sicurezza

b) completezza

c) esattezza

d) accessibilità

e) legittimità e conformità ai principi di pertinenza, non eccedenza, temporaneità ed indispensabilità rispetto alle finalità perseguite.

Laddove documenti, dati e informazioni, oggetto di pubblicazione obbligatoria per finalità di trasparenza, contengano dati personali, questi ultimi devono essere oscurati, tranne deroghe previste da specifiche disposizioni.

Salva diversa disposizione di legge, il Titolare garantisce la riservatezza dei dati sensibili in sede di pubblicazione all'Albo on line o sulla rete civica, mediante la non identificabilità dei soggetti cui tali dati si riferiscono, adottando gli opportuni accorgimenti in sede di predisposizione degli atti stessi e dei relativi allegati. A tal fine, il Titolare adotta e implementa adeguate misure organizzative, di gestione documentale e di formazione.

Le misure organizzative per la gestione dei dati sono contenute nelle schede dei trattament.

In ogni caso, i documenti, soggetti a pubblicazione, riportanti informazioni di carattere sensibile o giudiziario dell'interessato, devono essere anonimizzati con adeguate tecniche di anonimizzazione.

I dati sensibili e giudiziari sono sottratti all'indicizzazione e alla rintracciabilità tramite i motori di ricerca web esterni ed il loro riutilizzo.

Art. 18 – Diritto di accesso alla documentazione, diritto di accesso civico e protezione dei dati personali

I presupposti, le modalità, i limiti per l'esercizio del diritto di accesso ai documenti amministrativi e del diritto di accesso civico, semplice e generalizzato, contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla normativa in materia di accesso agli atti e di accesso civico.

Quando il trattamento concerne dati genetici, relativi alla salute, all'orientamento sessuale, il trattamento è consentito solo se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso è di rango almeno pari ai diritti dell' interessato ovvero consiste in un diritto della personalità o altro diritto o libertà fondamentale.

Art. 19 – Diritti dell'interessato

Il Titolare attua e implementa le misure organizzative, gestionali, procedurali e documentali necessarie a facilitare l'esercizio dei diritti dell'interessato, di seguito elencati, in conformità alla disciplina contenuta nel GDPR e nel Codice.

I diritti delle persone decedute possono essere esercitati da chi ha un interesse proprio o per ragioni familiari meritevoli di protezione, se l' interessato non l'aveva vietato in modo non equivoco.

In ogni caso l' eventuale divieto non può ledere diritti patrimoniali di terzi derivanti dalla morte dell' interessato.

Art. 20 – Diritto di accesso

Il presente Regolamento 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 finalità 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 è 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'autorità 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, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

I diritti dell' interessato possono essere limitati qualora dall' esercizio degli stessi possa derivare pregiudizio agli interessi tutelati dalle norme anti-riciclaggio, dalle disposizioni in materia di sostegno alle vittime delle condotte estorsive, dalle norme sul controllo del sistema dei pagamenti ovvero quando possano compromettere indagini difensivi o l' esercizio di diritti in sede giudiziario e la riservatezza del dipendente che segnala un illecito.

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 può 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 non deve ledere i diritti e le libertà altrui.

Art. 21 – Diritto alla rettifica e cancellazione

Il presente Regolamento tiene conto della disciplina del GDPR in tema di diritto di rettifica e cancellazione («diritto all'oblio»), 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 finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Il Titolare comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato.

Quanto al diritto "all'oblio", consistente nel diritto di ottenere dal Titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo, lo stesso non si applica nella misura in cui il trattamento sia necessario:

- per l'esercizio del diritto alla libertà di espressione e di informazione;
- per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;
- per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3 GDPR;
- a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1 GDPR, nella misura in cui il diritto all'oblio rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o
- per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Art. 22 – Diritto alla limitazione

Il presente Regolamento 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 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 per verificare l'esattezza di tali dati personali;

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

c) benché il Titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;

d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1 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 è limitato a norma del paragrafo 1 dell'art. 18 GDPR, 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 è informato dal Titolare 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 ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il Titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

Art. 23 – Diritto alla portabilità

Il presente Regolamento tiene conto della circostanza che, in forza della disciplina del GDPR, il diritto alla portabilità dei dati non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento.

Art. 24 – 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 libertà 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 dell'art. 21 GDPR è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.

Nel contesto dell'utilizzo di servizi della società dell'informazione e fatta salva la direttiva 2002/58/CE, l'interessato può 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 del 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 è necessario per l'esecuzione di un compito di interesse pubblico.

Art. 25 – Modalità di esercizio dei diritti dell'interessato

Per l'esercizio dei diritti dell'interessato, in ordine all'accesso ed al trattamento dei suoi dati personali, si applicano le disposizioni del GDPR, del Codice e del presente Regolamento.

La richiesta per l'esercizio dei diritti può essere fatta pervenire:

- direttamente dall'interessato, anche facendosi assistere da una persona di fiducia, con l'esibizione di un documento personale di riconoscimento o allegandone copia o anche con altre adeguate modalità o in presenza di circostanze atte a dimostrare l'identità personale dell'interessato stesso, come ad esempio, la conoscenza personale;

- tramite altra persona fisica o associazione, a cui abbia conferito per iscritto delega o procura; in tal caso, la persona che agisce su incarico dell'interessato deve consegnare copia della procura o della delega, nonché copia fotostatica non autenticata di un documento di riconoscimento del sottoscrittore;

- tramite chi esercita la potestà o la tutela, per i minori e gli incapaci;

- in caso di persone decedute, da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione;

- dalla persona fisica legittimata in base ai relativi statuti od ordinamenti, se l'interessato è una persona giuridica, un ente o un'associazione.

L'interessato può presentare o inviare la richiesta di esercizio dei diritti:

- al Titolare o Responsabile del trattamento, che conserva e gestisce i dati personali dell'interessato;

- all'ufficio protocollo generale del Titolare o all'ufficio per le relazioni con il pubblico.

La richiesta, per l'esercizio dei diritti di accesso ai dati personali, può essere esercitata dall'interessato solo in riferimento:

- alle informazioni che lo riguardano e non ai dati personali relativi ai terzi, eventualmente presenti all'interno dei documenti che lo riguardano.

Fermo restando l'accesso ai dati personali, il Resaponsabile. autorizza l'esibizione degli atti all'interessato, ricorrendo le condizioni per l'accesso.

I soggetti competenti alla valutazione dell'istanza sono:

- il Responsabile competente;

il quale decide sull'ammissibilità della richiesta d'accesso e sulle modalità di accesso ai dati.

All'istanza deve essere dato riscontro entro 30 giorni dalla data di ricezione della stessa.

I termini possono essere prolungati ad altri 30 giorni dalla data di ricezione, previa tempestiva comunicazione all'interessato, qualora l'istanza avanzata dal richiedente sia di particolare complessità o ricorra un giustificato motivo.

L'accesso dell'interessato ai propri dati personali:

- può essere differito limitatamente al periodo strettamente necessario durante il quale i dati stessi sono trattati esclusivamente per lo svolgimento di indagini difensive o per salvaguardare esigenze di riservatezza del Titolare. L'accesso è tuttavia

consentito agli altri dati personali dell'interessato che non incidono sulle ragioni di tutela a base del differimento.

Art. 26 – Indagini difensive

Ai fini delle indagini svolte nel corso di un procedimento penale, il difensore, ai sensi della Legge 7 dicembre 2000, n. 397 e dell'art. 391-quater del Codice di procedura penale, può chiedere documenti in possesso del Titolare, e può estrarne copia, anche se contengono dati personali di un terzo interessato.

Il rilascio è subordinato alla verifica che il diritto difeso sia di rango almeno pari a quello dell'interessato, e cioè consistente in un diritto della personalità o in un altro diritto o libertà fondamentale ed inviolabile rinviando, per ogni altro e ulteriore aspetto, alla relativa disciplina al Regolamento del Titolare sul diritto di accesso.

CAPO V – SOGGETTI

Art. 27 – Titolare e contitolari

Il Titolare del trattamento è il Comune di Andora, rappresentato dal Sindaco pro tempore, in qualità di legale rappresentante del Titolare, con sede in via Cavour n. 94, 17051 Andora.

Il Titolare provvede:

- a definire gli obiettivi strategici per la protezione dei dati personali in ordine al trattamento, provvedendo all'inserimento di tali obiettivi strategici nel DUP e negli altri documenti di programmazione e pianificazione del Titolare;

- a mettere in atto misure tecniche e organizzative adeguate per garantire che il trattamento sia effettuato conformemente al Codice, al GDPR e al presente Regolamento;

- a delegare ovvero a nominare, con proprio atto, i Responsabili per i compiti, le funzioni e i poteri in ordine ai processi, procedimenti, e adempimenti relativi al trattamento dei dati personali, alla sicurezza e alla formazione, impartendo ad essi, le necessarie istruzioni, in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato, all'adozione delle misure di sicurezza per la conservazione, protezione e sicurezza dei dati, all'eventuale uso di apparecchiature di videosorveglianza;

- a formare e aggiornare l'elenco dei dirigenti/P.O., delegati o nominati, e a pubblicarlo sul sito web istituzionale del Titolare;

- a designare, con proprio atto, il Responsabile per la Protezione dei Dati personali;

- a disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati e alla formazione dei dipendenti;

- a favorire l'adesione a codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi;

- a favorire l'adesione a meccanismi di certificazione;

- ad assolvere agli obblighi nei confronti del Garante nei casi previsti dalla vigente normativa.

Art. 28 – Dirigenti e Responsabili di Posizione organizzativa - P.O.

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/ P.O.

Nel suddetto provvedimento, il Titolare deve informare ciascun dirigente/ P.O., delle responsabilità che gli sono affidate in relazione a quanto disposto dal Codice, dal GDPR e dal presente Regolamento.

Compiti, funzioni e poteri:

- trattare i dati personali solo su istruzione del Titolare del trattamento;

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

- adottare il tempestivo ed integrale rispetto dei doveri del Titolare previsti dal Codice, compreso il profilo relativo alla sicurezza del trattamento così come disciplinato nell'art. 32 del GDPR;

- osservare le disposizioni del presente Regolamento nonché delle specifiche istruzioni impartite dal Titolare;

- adottare idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dalla normativa vigente, dalle disposizioni del Garante, dalle disposizioni contenute nel presente Regolamento, con particolare riguardo a tutte le disposizioni di rango speciale che comunque incidono sul trattamento dei dati;

- collaborare con il Titolare del trattamento per la predisposizione del documento di valutazione d'impatto sulla protezione dei dati e per la definizione del Registro delle attività di trattamento, in collaborazione con l'amministratore di sistema e con le altre strutture competenti del Titolare, nonché per gli eventuali aggiornamenti o adeguamenti del documento stesso;

- curare l'elaborazione e la raccolta della modulistica e delle informative, da utilizzarsi all'interno dell'organizzazione del Titolare per l'applicazione del Codice, del GDPR, e del presente Regolamento;

- assistere il Titolare del trattamento con misure tecniche ed organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato per quanto previsto nella normativa vigente;

- assistere il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR (sicurezza del trattamento dei dati personali,

notifica di una violazione dei dati personali all'autorità di controllo, comunicazione di una violazione dei dati personali all'interessato, valutazione d'impatto sulla protezione dei dati, consultazione preventiva) tenendo conto della natura del trattamento e delle informazioni a disposizione;

- mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti nel Codice, GDPR e nel presente Regolamento;

- contribuire alle attività di verifica del rispetto del Codice, del GDPR e del presente regolamento, comprese le ispezioni, realizzate dal Titolare o da un altro soggetto da questi incaricato;

- curare la costituzione e l'aggiornamento dei seguenti archivi/banche dati, per quanto di competenza:

• elenco dei contitolari, dei responsabili dei trattamenti, e degli incaricati, con i relativi punti di contatto;

• elenco degli archivi/ banche;

- garantire l'aggiornamento della ricognizione dei trattamenti;

- fornire tutte le necessarie informazioni e prestare assistenza al Responsabile della protezione dei dati (RPD/PDO) nell'esercizio delle sue funzioni.

Ciascun dirigente/P.O., 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, nonché 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 modalità 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 del Titolare ed all'esterno, qualora agli stessi vi sia 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 Responsabile 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/P.O. sono destinatari degli interventi di formazione di aggiornamento.

Art. 29 – Responsabili del trattamento e sub responsabili

Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti. In particolare, il Titolare può avvalersi, per il trattamento di dati, anche sensibili, di soggetti pubblici o privati che, in qualità 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 è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

I Responsabili del trattamento hanno l'obbligo di:

- trattare i dati in modo lecito, secondo correttezza e nel pieno rispetto della normativa vigente in materia;

- rispettare le misure di sicurezza previste dal Codice sulla privacy e adottare tutte le misure che siano idonee a prevenire e/o evitare la comunicazione o diffusione dei dati, il rischio di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non autorizzato o non conforme alle finalità della raccolta;

- nominare al loro interno i soggetti incaricati del trattamento;

- garantire che i dati trattati siano portati a conoscenza soltanto del personale incaricato del trattamento;

- trattare i dati personali, anche di natura sensibile e sanitaria, dei Pazienti esclusivamente per le finalità previste dal contratto o dalla convenzione;

- attenersi alle disposizioni impartite dal Titolare del trattamento;

- specificare i luoghi dove fisicamente avviene il trattamento dei dati e su quali supporti;

- comunicare le misure minime di sicurezza adottate per garantire la riservatezza e la protezione dei dati personali trattati.

L'accettazione della nomina e l'impegno a rispettare le disposizioni del Codice, del GDPR e del presente Regolamento è condizione necessaria per l'instaurarsi del rapporto giuridico fra le parti.

Art. 30 – Incaricati del trattamento dipendenti del Titolare

Gli incaricati del trattamento sono le persone fisiche, dipendenti del Titolare, designati da ciascun dirigente/P.O., 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 modalità.

La designazione dell'incaricato al trattamento dei dati personali è di competenza del dirigente/P.O.; la nomina è effettuata per iscritto e individua specificatamente i compiti spettanti all'incaricato e le modalità cui 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'unità per la quale risulti individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità 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, è da considerare, "incaricato" ai sensi dell'art. 30 del Codice nonché ai sensi degli artt. 4 comma 10 e art. 28 comma 3 del GDPR.

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

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

In particolare, gli incaricati devono assicurare che, nel corso del trattamento, i dati siano:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;

- raccolti e registrati per scopi determinati, espliciti e legittimi, e successivamente trattati in modo compatibile con tali finalità;

- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;

- esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;

- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore a quello necessario per il conseguimento delle finalità per le quali i dati sono trattati;

- trattati in modo tale che venga ad essere garantita un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure organizzative e tecniche adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale.

Gli incaricati sono tenuti alla completa riservatezza sui dati di cui siano venuti a conoscenza in occasione dell'espletamento della propria attività, impegnandosi a comunicare i dati esclusivamente ai soggetti indicati dal Titolare e dal dirigente/P.O., nei soli casi previsti dalla legge, nello svolgimento dell'attività istituzionale del Titolare.

Gli incaricati dipendenti del Titolare sono destinatari degli interventi di formazione di aggiornamento.

Art. 31 – Incaricati del trattamento non dipendenti del Titolare soggetti esterni

Tutti i soggetti che svolgono un'attività di trattamento dei dati, e che non sono dipendenti del Titolare, quali a titolo meramente esemplificativo i tirocinanti, i volontari e i soggetti che operano temporaneamente all'interno della struttura

organizzativa del Titolare , devono essere incaricati del trattamento tramite atto scritto di nomina.

Questi ultimi sono soggetti agli stessi obblighi cui sono sottoposti tutti gli incaricati dipendenti del Titolare, in modo da garantire il pieno rispetto della tutela della riservatezza dei dati.

Gli incaricati non dipendenti dal Titolare sono destinatari degli interventi di formazione di aggiornamento.

Art. 32 – Amministratore di sistema

L'amministratore di sistema, individuato nel Responsabile del Centro Elaborazione Dati, sovraintende alla gestione e alla manutenzione delle banche dati e, nel suo complesso, al sistema informatico di cui è dotata l'Amministrazione.

L'amministratore di sistema svolge attività, quali:

- il salvataggio dei dati, l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware e propone al Titolare del trattamento un documento di valutazione del rischio informatico.

Nel rispetto della normativa in materia di protezione dei dati e della sicurezza, l'amministratore di sistema:

- deve adottare sistemi idonei alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici. Le registrazioni (access log) devono essere complete, inalterabili, verificabili nella loro integrità, e adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

Le registrazioni devono comprendere il riferimento temporale e la descrizione dell'evento che le ha generate e devono essere conservate per un periodo congruo, non inferiore ai sei mesi.

Secondo la normativa vigente, l'operato dell'amministratore di sistema deve essere verificato, con cadenza annuale, da parte del Titolare del trattamento, in modo da controllare la rispondenza alle misure tecnico-organizzative e di sicurezza attivate rispetto all'attività di trattamento dei dati personali.

Il Titolare di sistema applica le disposizioni impartite dal Garante in materia di misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema.

L'amministratore di sistema è destinatario degli interventi di formazione di aggiornamento.

Art. 33 – Responsabile della Protezione dei Dati personali (RPD) – Data Protection Officer (DPO)

Il Titolare designa il Responsabile della protezione dei dati (RPD) che deve essere in possesso di:

- un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali;

- deve adempiere alle sue funzioni in totale indipendenza e in assenza di conflitti di interesse;

- operare alle dipendenze del Titolare del trattamento oppure sulla base di un contratto di servizio. Il RPD/PDO è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti.

Il Titolare del trattamento mette a disposizione del DPO le risorse necessarie per adempiere ai suoi compiti e accedere ai dati personali e ai trattamenti.

Il RPD/PDO svolge i seguenti compiti:

- informa e fornisce consulenze al Titolare del trattamento, nonché ai dipendenti che eseguono il trattamento dei dati in merito agli obblighi vigenti relativi alla protezione dei dati;

- verifica l'attuazione e l'applicazione della normativa vigente in materia, nonché delle politiche del Titolare o del Responsabile del trattamento relative alla protezione dei dati personali, inclusi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento, e gli audit relativi;

- fornisce, qualora venga richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorveglia i relativi adempimenti;

- funge da punto di contatto per gli interessati in merito al trattamento dei loro dati personali e all'esercizio dei diritti;

- funge da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento dei dati, tra cui la consultazione preventiva.

CAPO VI – SICUREZZA DEI DATI PERSONALI

Art. 34 – Misure di sicurezza

Il Titolare, nel trattamento dei dati personali, garantisce l'applicazione di adeguate e misure di sicurezza che consentono di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta.

In particolare il Titolare del trattamento mette in atto misure e tecniche, organizzative, di gestione, procedurali e documentali adeguate per garantire un livello di sicurezza adeguato al rischio. Tali misure che comprendono almeno:

- la pseudonimizzazione e la cifratura dei dati personali trattati;

- procedure per assicurare, in modo permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

- modalità per garantire il ripristino tempestivo nell'accesso ai dati personali in caso di incidente fisico o tecnico;

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

Per quanto attiene al trattamento dei dati personali effettuato con strumenti elettronici e non, il Titolare applica le misure minime disciplinate dagli articoli da 33 a 36 del Codice, nonché le ulteriori misure di sicurezza ritenute adeguate in riferimento al proprio contesto.

Art. 35 – Valutazione d'impatto sulla protezione dei dati (Data Protection Impact Analysis)

La valutazione d'impatto sulla protezione dei dati è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli.

La valutazione è uno strumento importante per la responsabilizzazione in quanto sostiene il Titolare non soltanto nel rispettare i requisiti del GDPR, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del medesimo GDPR.

La DPIA sulla protezione dei dati personali viene realizzata, prima di procedere al trattamento, dal Titolare del trattamento quando un tipo di trattamento, considerata la natura, il contesto, le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate (a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono magari trattati dati sensibili, o anche per una combinazione di questi e altri fattori), il regolamento 2016/679 obbliga i titolari a svolgere una valutazione di impatto prima di darvi inizio, consultando l´autorità di controllo in caso le misure tecniche e organizzative da loro stessi individuate per mitigare l´impatto del trattamento non siano ritenute sufficienti - cioè, quando il rischio residuale per i diritti e le libertà degli interessati resti elevato.

La valutazione di impatto costituisce una buona prassi al di là dei requisiti di legge, poiché attraverso di essa il Titolare può ricavare indicazioni importanti e utili a prevenire incidenti futuri ma non è richiesta nei seguenti casi:

- quando, sulla base di predetti criteri, risulta che il trattamento non è tale da "presentare un rischio elevato per i diritti e le libertà delle persone fisiche";
- quando la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono molto simili a un trattamento per il quale è 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'autorità 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 già stata effettuata una valutazione d'impatto sulla protezione dei dati nel contesto dell'adozione di tale base giuridica (articolo 35, paragrafo 10 GPDR);

° quando il trattamento è tra quelli già mappati nelle schede allegate.

Qualora eseguita la valutazione deve contenere :

• una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal Titolare del trattamento;

• una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

• una valutazione dei rischi per i diritti e le libertà degli interessati;

• 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 conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento, il Titolare del trattamento, se necessario, procede a un riesame della valutazione d'impatto sulla protezione dei dati.

Il Titolare del trattamento, nello svolgere l'attività di valutazione, si consulta con il Responsabile della protezione dei dati. Laddove la DPIA riveli la presenza di rischi residui elevati, il Titolare è tenuto a richiedere la consultazione preventiva dell'autorità di controllo in relazione al trattamento ai sensi dell' art. 36, paragrafo 1 GDPR.

Art. 36 – Pubblicazione sintesi della valutazione d'impatto

Il Titolare effettua la pubblicazione della valutazione o di una sintesi della stessa al fine di contribuire a stimolare la fiducia nei confronti dei trattamenti effettuati dal Titolare, nonché di dimostrare la responsabilizzazione e la trasparenza.

La DPIA pubblicata non deve contenere l'intera valutazione qualora essa possa presentare informazioni specifiche relative ai rischi per la sicurezza per il Titolare o divulgare segreti commerciali o informazioni commerciali sensibili. In queste circostanze, la versione pubblicata potrebbe consistere soltanto in una sintesi delle principali risultanze della DPIA o addirittura soltanto in una dichiarazione nella quale si afferma che la DPIA è stata condotta.

Art. 37 – Consultazione preventiva

Il Titolare, prima di procedere al trattamento dei dati, consulta, per il tramite del RPDil Garante qualora la valutazione d'impatto sulla protezione dei dati abbia evidenziato che il trattamento potrebbe presentare un rischio elevato in assenza di misure adottate.

Art. 38 – Modulistica e procedure

Il Titolare, al fine di agevolare e semplificare la corretta e puntuale applicazione delle disposizioni del Codice, del GDPR, del presente Regolamento, e di tutte le linee guida e provvedimenti del Garante

a) adotta e costantemente aggiorna:

- modelli uniformi di informativa;
- modelli e formule uniformi necessarie per gestire il trattamento dei dati e le misure di sicurezza;

b) elabora, approva, e costantemente aggiorna:

- adeguate procedure gestionali, da raccogliere in un apposito Manuale delle procedure.

Art. 39 – Responsabilità in caso di violazione delle disposizioni in materia di protezione dei dati personali

Il mancato rispetto delle disposizioni in materia di riservatezza dei dati personali è sanzionato con le sanzioni previste dagli articoli da 166 a 172 del Codice da parte del Garante, nonché con sanzioni di natura disciplinare.

Il Titolare del trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento.

Il Responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto agli obblighi previsti nel Codice nel GDPR e nel presente regolamento, e a lui specificamente diretti o ha agito in modo difforme o contrario rispetto alle legittime istruzioni impartitegli dal Titolare del trattamento.

Il Titolare e il Responsabile del trattamento sono esonerati da responsabilità se dimostrano che l'evento dannoso non è in alcun modo loro imputabile.

Art. 40 – Tutela amministrativa.

L' interessato che ritiene che i suoi diritti siano stati lesi può proporre reclamo al Garante o ricorso all' autorità giudiziaria.

I rimedi sono alternativi, non potendo essere proposti per il medesimo oggetto.

Il reclamo al Garante deve contenere

a) la descrizione della natura della violazione dei dati personali

b) il nome e i dati di contatto del Titolare e del Responsabile del trattamento;

c) la sottoscrizione in proprio o da parte di un ente del terzo settore che sia attivo per la tutela dei diritti e delle libertà con riguardo al trattamento dei dati personali;

d) allegare ogni documentazione utile.

Il reclamo deve essere deciso nel termine di mesi nove dalla presentazione, elevabili a dodici in presenza di motivate esigenze istruttorie.

Il Garante può adottare provvedimenti da pubblicare in Gazzetta Ufficile qualora i destinatari non siano identificabili.

Avverso le decisioni del Garante è ammesso ricorso giurisdizionale.

Al Garante possono altresì essere indirizzate segnalazioni per l'adozione di provvedimenti d'ufficio.

Art. 41 – Tutela giurisdizionale.

Le controversie riguardanti l'applicazione della normativa in materia di protezione dei dati personali sono attribuite al giudice ordinario e disciplinate dal Decreto legislativo 1 settembre 2011 n. 150.

Art. 42 – Disposizioni finali

Per quanto non previsto nel presente Regolamento si applicano le disposizioni del Codice, del GDPR, e i provvedimenti del Garante.

Il presente Regolamento è aggiornato a seguito di ulteriori modificazioni alla vigente normativa in materia di riservatezza e protezione dei dati personali.