(allegato alla deliberazione n. 218 del 28.12.2018)

Regolamento per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali

Art. 1
Oggetto

1. Il presente Regolamento ha per oggetto misure procedimentali e regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento europeo (General Data Protection Regulation) del 27 aprile 2016 n. 679, di seguito indicato "RGPD", Regolamento Generale Protezione Dati, relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati in ARPA Lazio (Agenzia regionale per la protezione ambientale del Lazio).
2. I dati personali sono trattati secondo quanto disposto dal presente Regolamento nonché dal Regolamento della Regione Lazio 30.04.2014, n. 11 (Trattamento dei dati sensibili e giudiziari di competenza della Giunta regionale, delle aziende Unità sanitarie locali, degli enti dipendenti e delle

agenzie regionali, delle società e degli altri enti privati a partecipazione regionale ai sensi degli artt. 20-21 del D.Lgs 196/03), in quanto applicabile.

Art.2

Disposizioni generali

1. Qualunque trattamento di dati personali da parte dell'ARPA Lazio è consentito soltanto per lo svolgimento delle funzioni istituzionali o gestionali correlate. Nel trattare i dati l'ARPA Lazio osserva i presupposti e i limiti stabiliti dal vigente codice in materia di protezione dei dati personali di cui al decreto legislativo 30.06.2003, n. 196 e s.m.i. , anche in relazione alla diversa natura dei dati, dalla legge e dai regolamenti vigenti. Il trattamento dei dati avviene nel rispetto dei diritti e delle libertà fondamentali dell'interessato ed è compiuto quando, per lo svolgimento delle finalità di interesse pubblico perseguito dall'ARPA Lazio, non è possibile il trattamento dei dati anonimi oppure di dati personali non sensibili o non giudiziari.
2. Il trattamento dei dati personali di cui l'ARPA Lazio è Titolare avviene nel rispetto e a garanzia dei principi di cui all'art. 5 del RGPD.

Art.3

Definizioni

1. Ai fini dell'applicazione delle norme di legge a tutela delle persone e di altri soggetti rispetto al trattamento e alla protezione dei dati personali, si definisce come:

   a) **dato personale**: qualsiasi informazione riguardante una persona fisica identificata o identificabile "interessato"; si considera identificabile la persona fisica che può essere identificata direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

   b) **dato sensibile**: ogni particolare informazione che concerne la sfera personale dei singoli che rilevi: origine razziale o etnica; opinioni politiche; convinzioni religiose o filosofiche; appartenenza sindacale; stato di salute; vita e orientamento sessuale; dati genetici; dati biometrici intesi a identificare in modo univoco una persona fisica;

   c) **trattamento dei dati**: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme 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;

   d) **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;

   e) **titolare del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;

   f) **responsabile del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.
2. I dati trattabili sono esclusivamente quelli essenziali per lo svolgimento delle attività istituzionali dell'Ente, in particolare:

   a) qualora il trattamento sia previsto da una espressa ed esaustiva disposizione di legge;

   b) qualora si evidenzi una rilevante finalità di interesse pubblico, dopo individuazione della fattispecie, su richiesta dell'Amministrazione, effettuata dall'Autorità garante.

Art.4

Titolare del trattamento

1. L'ARPA Lazio, rappresentata ai fini previsti dal RGPD dal Direttore generale, è il Titolare del trattamento dei dati personali raccolti o no in banche dati, automatizzate o cartacee, di seguito indicato "Titolare". Le competenze del Titolare sono esercitate dal Direttore Generale dell'ARPA Lazio o da suo delegato formalmente individuato.
2. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 RGPD.
3. Il Titolare mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al RGPD. Le misure sono definite ai fini dell'applicazione efficace dei principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli da 15 a 22 del RGPD (diritto di accesso; diritto di rettifica; diritto alla cancellazione; diritto di limitazione; obbligo di notifica in caso di cancellazione o limitazione del trattamento; diritto alla portabilità; diritto di opposizione; processo decisionale automatizzato, relativo alla persone fisiche), nonché le comunicazioni e le informazioni a esso afferenti.
4. Il Titolare adotta misure appropriate per fornire all'interessato:
   a) le informazioni indicate dall'art. 13 RGPD (tra cui identità e dati di contatto del Titolare e, ove applicabile, del suo rappresentante; dati di contatto del Responsabile della protezione dati, ove applicabile; finalità e base giuridica del trattamento; eventuali legittimi interessi perseguiti dal Titolare o da terzi; eventuali destinatari o categorie di destinatari dei dati; periodo di conservazione; ove applicabile, l'intenzione del Titolare di trasferire i dati a un destinatario in un paese terzo o a un'organizzazione internazionale; diritti dell'interessato; esistenza di un processo decisionale automatizzato, compresa la profilazione), qualora i dati personali siano raccolti presso lo stesso interessato;
   b) le informazioni indicate dall'art. 14 RGPD (tra cui identità e dati di contatto del Titolare e, ove applicabile, del suo rappresentante; dati di contatto del Responsabile della protezione dati, ove applicabile; finalità e base giuridica del trattamento; categorie di dati personali; eventuali destinatari o categorie di destinatari dei dati; ove applicabile, l'intenzione del Titolare di trasferire i dati a un destinatario in un paese terzo o a un'organizzazione internazionale; periodo di conservazione; diritti dell'interessato; la fonte da cui hanno origine i dati personali; esistenza di un processo decisionale automatizzato, compresa la profilazione), qualora i dati personali non siano stati ottenuti presso lo stesso interessato.
5. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali, di seguito indicata "DPIA – Data Protection Impact Assessment", ai sensi dell'art. 35 del RGDP, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 12.
6. Il Titolare, inoltre, provvede a:
   a) designare i Responsabili del trattamento nelle persone dei responsabili di Unità Organizzative Complesse (U.O.C.) in cui si articola l'organizzazione nonché dei responsabili di Unità Organizzative Semplici (U.O.S.) alle dirette dipendenze della Direzione generale, che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza. Per il trattamento di dati il Titolare può avvalersi anche di soggetti pubblici o privati;
   b) nominare il Responsabile della protezione dei dati;
   c) nominare quale Responsabile del trattamento i soggetti pubblici o privati affidatari di attività e servizi per conto dell'ARPA Lazio, relativamente alle banche dati gestite da soggetti esterni all'ARPA Lazio in

virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali;

d) predisporre l'elenco dei Responsabili del trattamento delle strutture in cui si articola l'organizzazione, pubblicandolo in apposita sezione del sito istituzionale e aggiornandolo periodicamente.

Art.5

Responsabile del trattamento

1. I Dirigenti responsabili di Unità Organizzative Complesse (U.O.C.) nonché i Dirigenti responsabili delle Unità Organizzative Semplici (U.O.S.) alle dirette dipendenze della Direzione generale, sono nominati Responsabili del trattamento di tutte le banche dati personali esistenti nell'articolazione organizzativa di rispettiva competenza. Il Responsabile del trattamento deve essere in grado di offrire garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità e affidabilità, per mettere in atto le misure tecniche e organizzative di cui all'art. 9 rivolte a garantire che i trattamenti siano effettuati in conformità al RGPD.
2. I dipendenti dell'ARPA Lazio Responsabili del trattamento, sono nominati, di norma, mediante deliberazione di conferimento incarico del Direttore generale nella quale sono tassativamente disciplinati:
   a) la materia trattata, la durata, la natura e la finalità del trattamento o dei trattamenti assegnati;
   b) il tipo di dati personali oggetto di trattamento e le categorie di interessati;
   c) gli obblighi e i diritti del Titolare del trattamento.
3. 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 di cui al paragrafo 1, stipulando atti giuridici in forma scritta, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del responsabile del trattamento e le modalità di trattamento.
4. Gli atti che disciplinano il rapporto tra il Titolare e il Responsabile del trattamento devono in particolare contenere quanto previsto dall'art. 28, paragrafo 3, del RGPD; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.
5. Il Responsabile del trattamento garantisce che chiunque agisca sotto la sua autorità e abbia accesso a dati personali sia in possesso di apposita formazione e istruzione e si sia impegnato alla riservatezza o abbia un adeguato obbligo legale di riservatezza.
6. Il Responsabile del trattamento dei dati provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti affidatigli dal Titolare, analiticamente specificati per iscritto nell'atto di nomina e in particolare provvede:
   a) alla tenuta del registro delle categorie di attività di trattamento svolte per conto del Titolare;
   b) all'adozione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti;
   c) alla sensibilizzazione e alla formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
   d) alla nomina dei sub-responsabili;
   e) ad assistere il Titolare nella conduzione della valutazione dell'impatto sulla protezione dei dati, fornendo allo stesso ogni informazione di cui è in possesso;
   f) a informare ai sensi dell'art. 13 il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali, cd. "*data breach*", per la successiva notifica della violazione al Garante Privacy, nel caso che il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati.

Art.6

Responsabile della protezione dati

1. Il Responsabile della protezione dei dati, in seguito indicato "RPD", svolge un ruolo chiave nella promozione della cultura della protezione dei dati all'interno dell'ARPA Lazio e contribuisce a dare attuazione a quanto previsto dal RGPD in relazione ai principi fondamentali del trattamento, ai diritti degli interessati, alla protezione dei dati sin dalla fase di progettazione, ai registri di trattamento, alla sicurezza dei trattamenti nonché alla notifica e comunicazione delle violazione di dati personali.
2. Il RDP dell'ARPA Lazio è individuato tramite procedura a evidenza pubblica.
3. Il RPD è incaricato dei seguenti compiti:
   a) informare e fornire consulenza al Titolare e al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD e dalle altre normative relative alla protezione dei dati. In tal senso il RPD può indicare al Titolare e/o al Responsabile del trattamento i settori funzionali ai quali riservare un *audit* interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali, e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;
   b) sorvegliare l'osservanza del RGPD e delle altre normative relative alla protezione dei dati, ferme restando le responsabilità del Titolare e del Responsabile del trattamento. Fanno parte di questi compiti la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare e del Responsabile del trattamento;
   c) sorvegliare in ordine alle attribuzioni di responsabilità, alle attività di sensibilizzazione, alla formazione e controllo poste in essere dal Titolare e dal Responsabile del trattamento;
   d) fornire, se richiesto, un parere in merito alla DPIA e sorvegliarne lo svolgimento;
   e) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 RGPD ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del RPD è comunicato dal Titolare e/o dal Responsabile del trattamento al Garante;
   f) predisporre il registro delle attività di trattamento di cui al successivo art. 10;
   g) predisporre il registro delle categorie di attività di cui al successivo art. 11;
   h) verificare la tenuta dei registri del Titolare e dei Responsabili del trattamento;
   i) mappare i processi;
   j) altri compiti e funzioni a condizione che il Titolare o il Responsabile del trattamento si assicurino che tali compiti e funzioni non diano adito a un conflitto di interessi. L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del RPD.
4. Il Titolare e il Responsabile del trattamento assicurano che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:
   a) il RPD è invitato a partecipare alle riunioni di coordinamento dei Dirigenti Responsabili di U.O.C. che abbiano per oggetto questioni inerenti alla protezione dei dati personali;
   b) il RPD deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea, scritta od orale;
   c) il parere del RPD sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta determini condotte difformi da quelle raccomandate dal RPD, è necessario motivare specificamente tale decisione;
   d) il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente connesso al trattamento di dati personali.

5. Nello svolgimento dei compiti affidatigli il RPD deve debitamente considerare i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo. In tal senso il RPD:
   a) procede a una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati;
   b) definisce un ordine di priorità nell'attività da svolgere - ovvero un piano annuale di attività - incentrandola sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati, da comunicare al Titolare e al Responsabile del trattamento.
6. Il RPD dispone di autonomia e risorse sufficienti a svolgere in modo efficace i compiti attribuiti, tenuto conto delle dimensioni organizzative e delle capacità di bilancio dell'ARPA Lazio.
7. La figura di RPD è incompatibile con chi determina le finalità o i mezzi del trattamento; in particolare, risultano con la stessa incompatibili:
   a) il Responsabile per la prevenzione della corruzione e per la trasparenza;
   b) il Responsabile del trattamento;
   c) qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.
8. Il RPD opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti; in particolare, non deve ricevere istruzioni in merito al loro svolgimento né all'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati. Il RPD non può essere rimosso o penalizzato dal Titolare e dal Responsabile del trattamento per l'adempimento dei propri compiti. Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare – Direttore generale o suo delegato - od al Responsabile del trattamento.

Art.7

Responsabile del trattamento

dei dati informatici e telematici (DIT)

1. La responsabilità del trattamento dei dati informatici e telematici è attribuita al Dirigente Responsabile dell'Unità Sviluppo dei sistemi informativi.
2. Il RDIT assicura:
   a) l'attività di controllo e gestione dei sistemi di elaborazione o di sue componenti, di base di dati, di reti, di apparati di sicurezza e di sistemi di software complessi;
   b) l'individuazione e attuazione di tutte le procedure fisiche, logiche e organizzative per tutelare la sicurezza e la riservatezza nel trattamento dei dati informatici.

Art.8

Consenso

1. L'ARPA Lazio per lo svolgimento dei propri compiti istituzionali non deve, di regola, chiedere il consenso per il trattamento dei dati personali.
2. Il Titolare, qualora il trattamento sia basato sul consenso, deve essere in grado di dimostrare che l'interessato ha espresso il proprio consenso al trattamento dei propri dati personali. Se il consenso dell'interessato è espresso nel contesto di una dichiarazione scritta, anche attraverso mezzi elettronici, che riguarda anche altre materie, la richiesta di consenso deve essere presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile.
3. 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.

Art.9

Sicurezza del trattamento

1. Il Titolare e ciascun Responsabile del trattamento mettono in atto misure tecniche e organizzative congrue per garantire un livello di sicurezza adeguato al rischio tenendo conto dello stato dell'arte e dei

costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

2. Le misure tecniche e organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento comprendono: la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
3. Costituiscono misure tecniche e organizzative che possono essere adottate dalle strutture cui è preposto ciascun Responsabile del trattamento:
   a) sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro);
   b) misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione di archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.
4. La conformità del trattamento dei dati al RGDP in materia di protezione dei dati personali è dimostrata attraverso l'adozione delle misure di sicurezza o l'adesione a codici di condotta approvati o a un meccanismo di certificazione approvato.
5. Il Titolare e ciascun Responsabile del trattamento si obbligano a impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto e abbia accesso a dati personali.
6. I nominativi e i dati di contatto del Titolare, dei Responsabili del trattamento e del Responsabile della protezione dati sono pubblicati sul sito istituzionale dell'ARPA Lazio, sezione Amministrazione trasparente, oltre che nella sezione "privacy".

Art.10

Registro delle attività di trattamento

1. Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca almeno le seguenti informazioni:
   a) il nome e i dati di contatto dell'ARPA Lazio, del Direttore generale o suo delegato, dei Responsabili del trattamento ai sensi del precedente art.5, dei Contitolari del trattamento e del RPD;
   b) le finalità del trattamento;
   c) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
   d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
   e) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
   f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
   g) il richiamo alle misure di sicurezza tecniche e organizzative del trattamento adottate, come da precedente art.9.
2. Il Registro è tenuto dal Titolare in forma digitale/cartacea, secondo lo schema allegato A al presente Regolamento; nello stesso possono essere inserite ulteriori informazioni tenuto conto delle dimensioni organizzative dell'ARPA Lazio.

Art.11

Registro delle categorie di attività trattate

1. Il Registro delle categorie di attività trattate da ciascun Responsabile del trattamento di cui al precedente art. 5, reca le seguenti informazioni:

a) il nome e i dati di contatto del Responsabile del trattamento e del RPD;
b) le categorie di trattamenti effettuati da ciascun Responsabile: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, raffronto, interconnessione, limitazione, cancellazione, distruzione, profilazione, pseudonimizzazione, ogni altra operazione applicata a dati personali;
c) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
d) il richiamo alle misure di sicurezza tecniche e organizzative del trattamento adottate, come da precedente art. 9.

2. Il registro è tenuto dal Responsabile del trattamento presso gli uffici della propria struttura organizzativa in forma telematica/cartacea, secondo lo schema allegato B al presente regolamento.

Art.12

Valutazioni d'impatto sulla protezione dei dati

1. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve attuare una DPIA ai sensi dell'art. 35 RGDP, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento. La DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.
2. Ai fini della decisione di effettuare o no la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante Privacy ai sensi dell'art. 35, paragrafi 4 e 6, RGDP.
3. La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. Fermo restando quanto indicato dall'art. 35, paragrafo 3, RGDP, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:
   a) trattamenti valutativi o di *scoring*, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;
   b) decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;
   c) monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;
   d) trattamenti, su larga scala, di dati sensibili o di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9 RGDP nonché di dati relativi a condanne penali e a reati di cui all'art. 10 RGDP;
   e) trattamenti di dati su larga scala, tenendo conto: del numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;
   f) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;
   g) dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento, come i dipendenti dell'Ente, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;

h) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;
i) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

4. Nel caso in cui un trattamento soddisfi almeno due dei criteri indicati al paragrafo 3 occorre, in via generale, condurre una DPIA, salvo che il Titolare ritenga motivatamente che non può presentare un rischio elevato; il Titolare può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.
5. Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della DPIA a un altro soggetto, interno o esterno all'ARPA Lazio. Il Titolare deve consultarsi con il RPD anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA. Il RPD monitora lo svolgimento della DPIA. Il Responsabile del trattamento deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria. Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, forniscono supporto al Titolare per lo svolgimento della DPIA.
6. Il RPD può proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale. Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, possono proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.
7. La DPIA non è necessaria nei casi seguenti:
   a) se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, paragrafo 1, RGDP;
   b) se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;
   c) se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche;
   d) se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.
8. Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o da un RDP e che proseguano con le stesse modalità oggetto di tale verifica. Inoltre, occorre tener conto che le autorizzazioni del Garante Privacy basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite o abrogate.
9. La DPIA è condotta prima di dar luogo al trattamento, attraverso i seguenti processi:
   a) descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati. Sono altresì indicati: i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei dati personali quali hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei;
   b) valutazione della necessità e proporzionalità dei trattamenti, sulla base:
   1) delle finalità specifiche, esplicite e legittime;
   2) della liceità del trattamento;
   3) dei dati adeguati, pertinenti e limitati a quanto necessario;
   4) del periodo limitato di conservazione;
   5) delle informazioni fornite agli interessati;

6) del diritto di accesso e portabilità dei dati;
7) del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
8) dei rapporti con i responsabili del trattamento;
9) delle garanzie per i trasferimenti internazionali di dati;
10) della consultazione preventiva del Garante privacy;

c) valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio, quale accesso illegittimo, modifiche indesiderate, indisponibilità dei dati, dal punto di vista degli interessati;

d) individuazione delle misure previste per affrontare e attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il RGPD, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

10. Il Titolare può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati. La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.
11. Il Titolare deve consultare il Garante Privacy prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato. Il Titolare consulta il Garante Privacy anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale e alla sanità pubblica.
12. La DPIA deve essere effettuata, con eventuale riesame delle valutazioni condotte, anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.
13. Sul sito istituzionale dell'ARPA Lazio viene pubblicata, in apposita sezione, una sintesi delle principali risultanze del processo di valutazione ovvero una semplice dichiarazione relativa all'effettuazione della DPIA.

Art. 13

Violazione dei dati personali

1. Per violazione dei dati personali, in seguito "*data breach*", si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dall'ARPA Lazio.
2. Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy. La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo. Il Responsabile del trattamento è obbligato a informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.
3. I principali rischi per i diritti e le libertà degli interessati conseguenti a una violazione, in conformità al considerando 75 del RGPD, sono i seguenti:
   a) danni fisici, materiali o immateriali alle persone fisiche;
   b) perdita del controllo dei dati personali;
   c) limitazione dei diritti, discriminazione;
   d) furto o usurpazione d'identità;
   e) perdite finanziarie, danno economico o sociale.
   f) decifratura non autorizzata della pseudonimizzazione;
   g) pregiudizio alla reputazione;

h) perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).

4. Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatasi. I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:
   a) coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
   b) riguardare le categorie particolari di dati personali sensibili di cui all'art. 9 RGDP;
   c) comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
   d) comportare rischi imminenti e con un'elevata probabilità di accadimento;
   e) impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).
5. La notifica deve avere il contenuto minimo previsto dall'art. 33 RGPD, e anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33.
6. Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze a esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante Privacy al fine di verificare il rispetto delle disposizioni del RGPD.

Art.14

Rinvio

1. Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le disposizioni del RGPD e tutte le sue norme attuative vigenti.

ALLEGATI

A) Registro attività di trattamento

B) Registro categorie di attività di trattamento