REGIONE
ABRUZZO

Disciplinare per l'attuazione del Regolamento in materia di protezione di dati personali (Reg. UE 2016/679)

REGIONE
ABRUZZO

INDICE:

Oggetto

Il presente Disciplinare detta misure organizzative e regole procedimentali di dettaglio ai fini dell'attuazione del Regolamento Europeo *General Data Protection Regulation* n. 679 del 2016 (di seguito indicato con "GDPR"), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati nella Giunta Regionale d'Abruzzo.

Il contenuto del presente Disciplinare deve intendersi quale direttiva puntuale ai fini dell'adeguamento, da parte dell'organizzazione amministrativa della Giunta Regionale d'Abruzzo, a quanto previsto dal "GDPR".
L'inosservanza di quanto previsto dal presente Disciplinare è valutata ai fini della responsabilità di cui all'articolo 21, commi 1 e 1-bis, del D.Lgs. 30.3.2001, n. 165 recante "*Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche*".

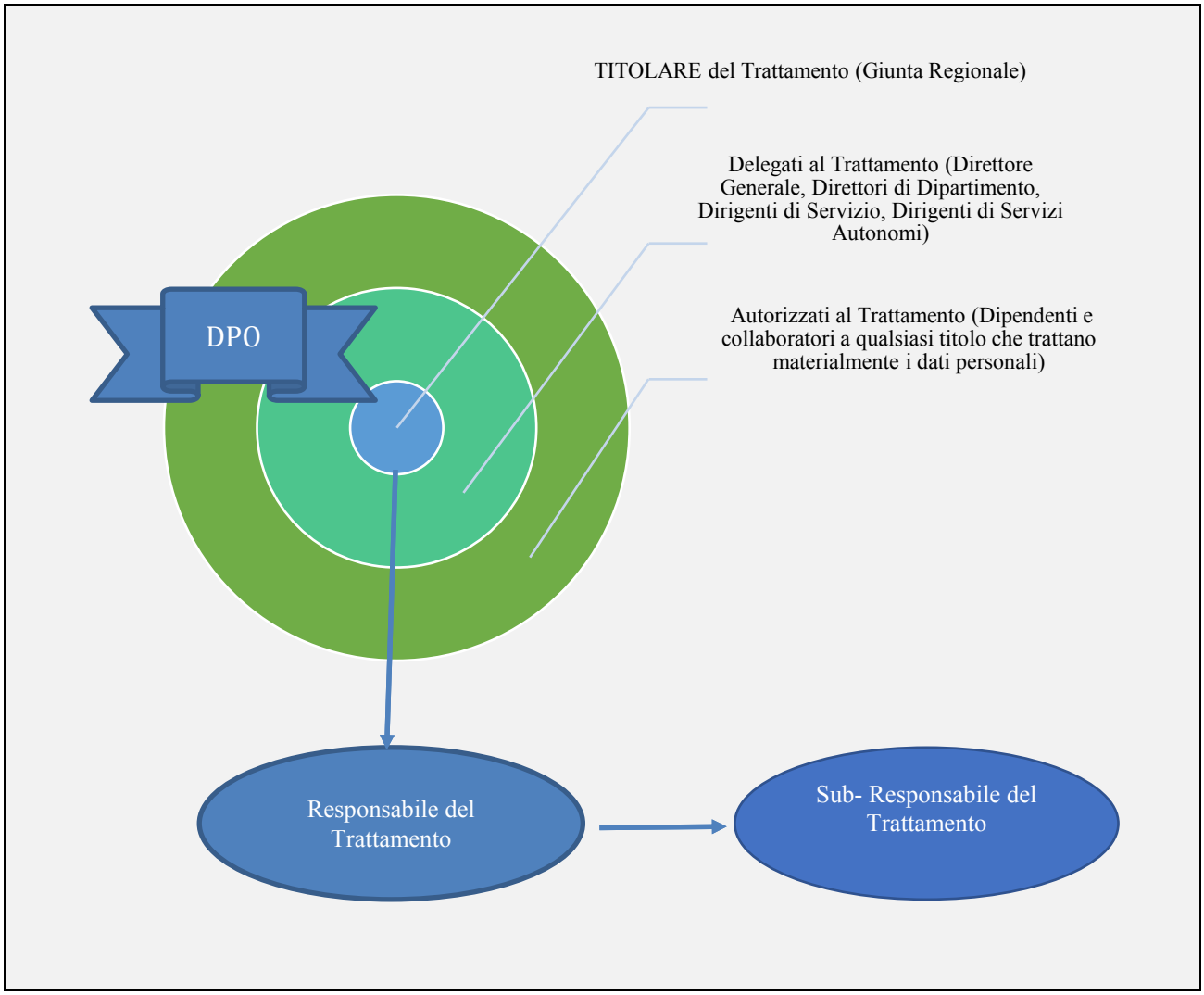
Organigramma privacy

Il "GDPR" impone che l'Ente, quale autorità pubblica, sia dotato di un preciso assetto organizzativo privacy.

A tal riguardo, in via generale, fatto salvo quanto successivamente previsto con riguardo ai Delegati al trattamento dei dati personali (paragrafo 1.2.1), la responsabilità della protezione dei dati personali nell'ambito dell'organizzazione amministrativa della Giunta Regionale d'Abruzzo è affidata alle Strutture organizzative di cui all'articolo 10, comma 1, lettere a), b), d) ed e) della Legge regionale 14 settembre 1999, n. 77 (*Norme in materia di organizzazione e rapporti di lavoro della Regione Abruzzo*), ciascuna secondo le rispettive competenze amministrative così come assegnate dalla Giunta Regionale per mezzo degli atti di macro e micro organizzazione.

Con riguardo alle strutture di supporto ai Componenti l'Esecutivo regionale la responsabilità della protezione dei dati personali è affidata alle strutture di cui all'articolo 26, comma 3, della Legge regionale 26 Agosto 2014, n. 35 (*Modifiche alla L.R. n. 77/1999 "Norme in materia di organizzazione e rapporti di lavoro della Regione Abruzzo", alla L.R. n. 9/2000 "Istituzione dell'Avvocatura regionale", alla L.R. n. 18/2001 "Consiglio regionale dell'Abruzzo, autonomia e organizzazione", alla L.R. n. 4/2009 "Principi generali in materia di riordino degli Enti regionali", parziale abrogazione della L.R. n. 17/2001 "Disposizioni per l'organizzazione ed il funzionamento delle strutture amministrative di supporto agli organi elettivi della Giunta regionale" e ulteriori disposizioni urgenti*).

Modello organizzativo privacy:



1. Soggetti del trattamento:

1.1. Titolare del Trattamento

Il Titolare del trattamento (*data controller*) è "*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*" (art. 4. par. 1, n. 7 GDPR).
Nel settore pubblico il titolare del trattamento è l'ente nel suo complesso.
Ai fini del presente Disciplinare la Giunta Regionale assume, a norma dell'art. 4, par. 1, punto 7 del GDPR, il ruolo di Titolare del trattamento**.**

1.2. Soggetti autorizzati al trattamento dei dati personali

L'art. 2-quaterdecies del Codice della Privacy ha introdotto la definizione di "soggetto autorizzato". In tal modo il titolare del trattamento o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente autorizzate, che operano sotto la loro autorità. Tale disposizione permette di mantenere le funzioni e i compiti assegnati a figure interne all'organizzazione.

Ai fini del presente disciplinare i soggetti autorizzati al trattamento si distinguono tra Delegati al trattamento dei dati personali (DAT) e Soggetti autorizzati al trattamento dei dati personali (SAT).

1.2.1. Delegati al trattamento dei dati personali (DAT)

Delegati al trattamento dei dati personali sono i titolari degli uffici di livello dirigenziale, comunque denominati, ai quali sono attribuiti, per mezzo dell'autorizzazione di cui alla sezione 2.1, i compiti e le funzioni stabiliti alla sezione 2.2, in quanto connessi al trattamento dei dati personali necessario allo svolgimento delle attività amministrative demandate ai medesimi Uffici.

Delegati al trattamento dei dati person**ali** sono altresì i soggetti posti in posizione di responsabilità nell'ambito delle strutture di supporto ai Componenti l'Esecutivo regionale, ai quali sono attribuiti, per mezzo dell'autorizzazione di cui alla sezione 2.1., i compiti e le funzioni stabiliti alla sezione 2.2, in quanto connessi al trattamento dei dati personali necessario allo svolgimento delle attività demandate alle medesime strutture.

1.2.2. Soggetti autorizzati al trattamento dei dati personali (SAT)

Soggetti autorizzati al trattamento dei dati personali (SAT**)** ai sensi dell'art. 4, par. 1, n. 10 GDPR, sono le persone fisiche che effettuano materialmente le operazioni di trattamento dei dati personali.

Ai fini del presente Disciplinare per Soggetti autorizzati al trattamento dei dati person**a**li si intendono sia i dipendenti regionali che qualunque altro soggetto autorizzato al trattamento dei dati personali, ai sensi di quanto previsto nella sezione 2.2, par. 1, lett. e), che operano sotto la responsabilità dei Delegati al trattamento dei dati personali.

1.3. Responsabile del trattamento

Responsabile del Trattamento, ai sensi dell'art. 28 GDPR (C81), è la persona fisica o giuridica, diversa dal Titolare ed esterna all'organizzazione dello stesso, che eventualmente effettua trattamenti per conto del Titolare. Il rapporto fra Titolare e Responsabile deve essere regolato da apposito contratto o altro atto bilaterale. Al Titolare spetta l'onere e la responsabilità di indicare al responsabile le modalità di trattamento e le relative istruzioni, nonché di controllare che le stesse siano rispettate.

1.4. Responsabile della protezione dati (RPD/DPO)

Il Responsabile della protezione dei dati (di seguito "RPD"), secondo quanto previsto agli artt. 37, 38 e 39 GDPR, svolge attività di promozione, consulenza e verifica circa la corretta applicazione del GDPR del Titolare del trattamento; mantiene altresì le relazioni con l'Autorità Garante e funge da punto di contatto con gli interessati per agevolare l'esercizio dei loro diritti.

2. FUNZIONI E COMPITI IN MATERIA DI TRATTAMENTO DEI DATI PERSONALI

2.1. Funzioni e compiti del Titolare del trattamento

1. Il Titolare del trattamento dei dati personali afferenti alle finalità dell'Ente Regione Abruzzo è la Giunta Regionale in persona del suo Presidente, la quale decide in ordine a finalità e mezzi dei trattamenti di propria competenza e ha la responsabilità di tenuta del registro dei trattamenti di cui all'art. 30 GDPR (C82).

2. Il Titolare è giuridicamente responsabile dell'ottemperanza agli obblighi previsti dalla normativa, sia nazionale che internazionale, in materia di protezione dei dati personali.

3. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali secondo quanto stabilito dall'art. 5 GDPR: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.

4. Il Titolare, tenuto conto di quanto previsto dall'articolo 2-quaterdecies del d.lgs. 30.06.2003 n.196, adempie ai propri compiti e funzioni connessi ai trattamenti dei dati personali attraverso i DAT, i quali operano sotto la sua autorità.

5. Il Titolare pone in atto misure tecniche e organizzative adeguate, al fine di garantire ed essere in grado di dimostrare che il trattamento dei dati personali sia effettuato in modo conforme al GDPR. Le misure sono definite fin dalla fase di progettazione, nel rispetto dei principi di protezione dei dati ed in maniera tale da agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli da 15 a 22 GDPR, tenuto conto, a tal fine, di quanto indicato nella successiva sezione 8. Gli interventi necessari per l'attuazione delle misure sono adottati previa analisi della situazione di fatto esistente, tenuto conto dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti per i diritti e le libertà delle persone fisiche, tenuto conto, a tal riguardo, del diverso grado di gravità e di probabilità che gli stessi possono presentare.

6. Il Titolare adotta misure appropriate per fornire all'interessato:
   a) le informazioni indicate dall'art. 13 GDPR, qualora i dati personali siano raccolti presso lo stesso interessato;
   b) le informazioni indicate dall'art. 14 GDPR, qualora i dati personali non siano raccolti presso lo stesso interessato.

7. Il Titolare, nel caso in cui un tipo di trattamento presenti un rischio elevato per i diritti e le libertà delle persone fisiche, deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA"), ai sensi dell'art. 35 GDPR, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato nella successiva sezione 6.

8. Il Titolare inoltre provvede a:

   a) designare i DAT nelle persone del Direttore Generale, dei Direttori di Dipartimento, dei Dirigenti preposti ad una Struttura Autonoma comunque denominata, dei Dirigenti preposti ad un Servizio e dei responsabili delle strutture di cui all'art. 26, comma 3, della legge regionale n. 35/2014, cui è affidato il trattamento dei dati nell'ambito delle attività di rispettiva competenza, nel rispetto della "*Procedura per la designazione dei Soggetti autorizzati al trattamento dei dati personali e relativa attribuzione di responsabilità*" così come riportata nell'Allegato A al presente Disciplinare;
   b) nominare il Responsabile della Protezione dei Dati (RPD);
   c) nominare il Responsabile del trattamento con riguardo al soggetto pubblico o privato affidatario di attività e servizi per conto della Giunta Regionale, relativamente al trattamento dei dati personali da parte di soggetti esterni, in virtù di convenzioni, contratti o incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali.

9. Il Titolare favorisce l'adesione ai codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi, ovvero a meccanismi di certificazione della protezione dei dati approvati, per contribuire alla corretta applicazione del GDPR e per dimostrarne il concreto rispetto da parte del Titolare del trattamento.

10. Ai fini di quanto previsto dal "GDPR" e dal presente disciplinare, i compiti e le funzioni proprie del Titolare**,** in quanto non espressamente delegate ai sensi delle successive sezioni 2.2. e 2.3., sono esercitate per il tramite di apposita struttura, diversa da quella cui è attribuito il ruolo di RPD, da individuarsi mediante successivo atto di organizzazione della Giunta Regionale.

2.2. Funzioni dei Delegati al trattamento dei dati personali (DAT)

I Delegati al trattamento dei dati personali (DA**T)**, sulla base dell'autorizzazione del Titolare, svolgono i compiti e le funzioni connesse al trattamento dei dati personali necessari ai fini del concreto svolgimento dell'attività amministrativa demandata alle strutture cui sono preposti.

1. A tal fine i DAT, nell'espletamento dei loro compiti e funzioni, sotto l'autorità del Titolare e con la collaborazione del RPD, provvedono a:
    a) stabilire, in maniera discrezionale, le finalità e le modalità di trattamento dei dati personali, acquisiti anche presso terzi, in quanto necessari all'espletamento delle funzioni amministrative di rispettiva competenza;
    b) tenere costantemente aggiornato il Registro informatizzato dei Trattamenti per la parte di rispettiva competenza;
    c) garantire il rispetto degli obblighi previsti dalla normativa, sia nazionale che internazionale, in materia di protezione dei dati personali;
    d) garantire il rispetto dei principi applicabili al trattamento dei dati personali secondo quanto stabilito dall'articolo 5 GDPR: liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza;
    e) autorizzare i SAT al trattamento dei dati personali ed a vigilare sulle istruzioni a tal fine impartite a mezzo della "*Procedura per la designazione dei Soggetti autorizzati al trattamento dei dati personali e relativa attribuzione di responsabilità*", relativamente al trattamento dei dati di rispettiva competenza;
    f) porre in atto misure tecniche e organizzative adeguate, al fine di garantire ed essere in grado di dimostrare che il trattamento di dati personali sia effettuato in modo conforme al GDPR. Le misure sono definite sin dalla fase di progettazione, nel rispetto dei principi di protezione dei dati ed in maniera tale da agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli da 15 a 22 GDPR, tenuto conto, a tal fine, di quanto indicato nella successiva sezione 8. Gli interventi necessari per l'attuazione delle misure sono adottati previa analisi della situazione di fatto esistente, tenuto conto dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi dallo stesso derivanti per i diritti e le libertà delle persone fisiche, tenuto conto, a tal riguardo, del diverso grado di gravità e di probabilità che gli stessi possono presentare;
    g) fornire all'interessato l'informativa di cui agli articoli 13 o 14 GDPR, verificandone il rispetto;
    h) effettuare, nel caso in cui un tipo di trattamento presenti un rischio elevato per i diritti e le libertà delle persone fisiche, una "DPIA", ai sensi dell'art. 35 GDPR, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato nella successiva sezione 6.

i) comunicare ogni notizia rilevante ai fini dell'osservanza degli obblighi dettati dagli articoli da 32 a 36 GDPR riguardanti l'adozione di misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio;
j) collaborare nella gestione delle istanze degli interessati;
k) informare il Titolare del trattamento, senza ingiustificato ritardo, della conoscenza dell'avvenuta violazione dei dati personali.

2.3. Compiti dei Soggetti autorizzati al trattamento dei dati personali (SAT)

1. I Soggetti autorizzati al trattamento dei dati personali (SAT) trattano i dati personali nella misura necessaria a raggiungere gli obiettivi relativi alle attività istituzionali svolte dalla struttura organizzativa di appartenenza. Le attività di trattamento dei dati personali sono correlate allo svolgimento delle proprie funzioni.

2. Il trattamento dei dati personali da parte dei SAT deve avvenire secondo le istruzioni impartite in sede di autorizzazione ovvero di quelle di volta in volta impartite per iscritto dal DAT, nel rispetto della "*Procedura per la designazione dei Soggetti autorizzati al trattamento dei dati personali e relativa attribuzione di responsabilità" (Allegato A)*.

3. Il SAT è tenuto a mantenere la riservatezza dei dati trattati.

4. Il SAT si impegna ad adottare le misure richieste dall'art. 32 GDPR secondo le istruzioni impartite.

2.4. Responsabile del trattamento dati

1. Qualora il Titolare decida di avvalersi di soggetti esterni per lo svolgimento di attività istituzionali, il DAT competente per la stipula del contratto o della convezione si avvale, per il trattamento dei dati anche appartenenti a categorie particolari (art. 9 GDPR), di soggetti che, in qualità di Responsabili del trattamento (RT), forniscano le garanzie di cui all'articolo 28, paragrafo 1 del GDPR.

2. Gli atti che disciplinano il rapporto tra il Titolare e il Responsabile del trattamento, la cui predisposizione compete al DAT, devono in particolare contenere quanto previsto dall'art. 28, paragrafo 3, del GDPR. Tali atti possono anche basarsi su clausole contrattuali tipo, anche sulla base di modelli predisposti dal Garante per la Protezione dei Dati Personali. A tal fine si tiene comunque conto di quanto previsto dalla "*Procedura per la gestione degli accordi di designazione del Responsabile del Trattamento*" (Allegato B).

3. È consentita la nomina di sub-responsabili del trattamento da parte di ciascun Responsabile del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano il Titolare e il Responsabile del Trattamento. Le operazioni di

trattamento possono essere effettuate solo da autorizzati che operano sotto la diretta autorità del Responsabile, attenendosi alle istruzioni loro impartite per iscritto, che individuino specificatamente l'ambito del trattamento consentito.

4. Il Responsabile risponde, anche dinanzi al Titolare, dell'operato del sub-responsabile anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non è in alcun modo allo stesso imputabile e che ha vigilato in modo adeguato sull'operato del sub-responsabile.

5. Il Responsabile del trattamento garantisce che chiunque agisca sotto la sua autorità e abbia accesso ai 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 ed a tutti i compiti affidatigli dal Titolare, analiticamente specificati per iscritto nell'atto di designazione, e in particolare provvede:
    a) alla tenuta ed all'aggiornamento del registro delle categorie di attività di trattamento svolte per conto del Titolare;
    b) all'adozione di idonee misure tecniche e organizzative adeguate al fine di garantire la sicurezza dei trattamenti;
    c) alla sensibilizzazione e alla formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
    d) ad assistere il Titolare nella conduzione della DPIA, fornendo allo stesso ogni informazione di cui è in possesso;
    e) ad informare 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 in cui il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati.

7. Uno o più DAT dell'ente Regione Abruzzo possono configurarsi, per conto della Giunta Regionale, come responsabili del trattamento per conto di un titolare diverso dalla Giunta Regionale d'Abruzzo[1].

[1] Es. il settore del personale che esegue per conto di altro Ente la gestione economica del personale in posizione di comando. Il dirigente del settore personale assume il ruolo e gli obblighi, a norma del GDPR, di Responsabile del trattamento nei confronti del Titolare dell'altro Ente.

2.5. Responsabile della protezione dei dati personali (RPD)

1. Il Responsabile della protezione dei dati (in seguito indicato con "RPD") è individuato nella figura unica di un dirigente di ruolo della Giunta Regionale d'Abruzzo, ovvero (in alternativa) di un professionista scelto tramite procedura ad evidenza pubblica.

2. Il RPD può essere scelto fra i Dirigenti della Giunta Regionale d'Abruzzo purché in possesso di idonee qualità professionali, con particolare riferimento alla comprovata conoscenza specialistica della normativa e della prassi in materia di protezione dei dati, nonché alla capacità di promuovere una cultura della protezione dati all'interno dell'organizzazione regionale. Il Titolare provvede affinché il RPD mantenga la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione.

3. Nel caso in cui il RPD non sia un dirigente dell'Ente, l'incaricato persona fisica è selezionato mediante procedura ad evidenza pubblica fra soggetti aventi le medesime qualità professionali richieste al dirigente, che abbiano maturato approfondita conoscenza del settore e delle strutture organizzative pubbliche di elevata complessità, nonché delle norme e procedure amministrative alle stessi applicabili. In tal caso i compiti attribuiti al RPD sono indicati in apposito contratto di servizi. Il RPD esterno è tenuto a mantenere la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione, con onere di comunicazione di detto adempimento al Titolare.

4. Il RPD è incaricato dei seguenti compiti:
    a) informare e fornire consulenza al Titolare ed ai DAT in merito agli obblighi derivanti dal GDPR e dalle altre normative in materia di protezione dei dati personali. In tal senso il RPD può indicare al Titolare e/o ai DAT 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, ed a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;
    b) sorvegliare l'osservanza del GDPR e delle altre normative relative alla protezione dei dati, ferme restando le responsabilità del Titolare. 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 dei delegati;
    c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dai DAT;
    d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento. Il Titolare, in particolare, si consulta con il RPD in merito a:
        - necessità di condurre o meno una DPIA;
        - quale metodologia adottare nel condurre una DPIA;

- opportunità di condurre la DPIA con le risorse interne ovvero esternalizzandola;
- indicazione delle salvaguardie da applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate;
- verifica sulla corretta effettuazione della DPIA e se le conclusioni raggiunte (procedere o meno con il trattamento e quali salvaguardie applicare) siano conformi al GDPR;

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 GDPR, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del RPD è comunicato dal Titolare al Garante;
f) verificare la corretta tenuta del Registro informatizzato dei trattamenti di cui alla successiva sezione 4;
g) altri compiti e funzioni a condizione che il Titolare e i DAT 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.

5. Il Titolare si assicura 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 Direttori/Dirigenti che abbiano per oggetto questioni che riguardano la 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 determina 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 (*Data Breach*).

6. 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 ad 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.

7. 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'Ente.

8. La figura di RPD è incompatibile con chi determina le finalità o i mezzi del trattamento. In particolare, risultano con la stessa incompatibili qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.

9. Il Titolare del trattamento fornisce al RPD le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali e ai trattamenti. In particolare è assicurato al RPD:
    a) supporto attivo per lo svolgimento dei compiti da parte dei Direttori/Dirigenti e della Giunta regionale;
    b) tempo sufficiente per l'espletamento dei compiti affidati al RPD;
    c) comunicazione ufficiale della nomina a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'Ente;
    d) accesso garantito ai settori funzionali dell'Ente così da fornirgli supporto, informazioni e input essenziali.

10. 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 sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati.

11. Il RPD non può essere rimosso o penalizzato dal Titolare per l'adempimento dei propri compiti.

12. Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare.

13. Nel caso in cui siano rilevate dal RPD o sottoposte alla sua attenzione decisioni incompatibili con il GDPR e con le indicazioni fornite dallo stesso RPD, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare.

14. L'Ufficio "Tutela della privacy" istituito in seno al Servizio Autonomo "Controlli e Anticorruzione", ai sensi della DGR n. 153/2020 è posto a supporto del RPD al fine di garantirne in modo adeguato la necessaria autonomia funzionale. A tal fine il medesimo Ufficio è ridenominato "Ufficio di supporto al RPD".

15. Il RPD della Giunta regionale, in collaborazione e in raccordo con la struttura di cui alla sezione 2.1.10, può procedere alla istituzione della rete dei referenti privacy anche nell'interesse del Titolare del Trattamento.

3. Sicurezza del trattamento

1. Il Titolare del trattamento, attraverso i DAT mette in atto misure tecniche e organizzative idonee a 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 probabilità e gravità per i diritti e le libertà delle persone fisiche.

2. Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono: la pseudominimizzazione; 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 ed organizzative che possono essere adottate dall'Ente:
    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 GDPR 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 ad un meccanismo di certificazione approvato.

5. Il livello di sicurezza è valutato tenuto conto dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. L'efficace protezione dei dati personali è perseguita sia al momento di determinare i mezzi del trattamento (fase progettuale) sia all'atto del trattamento.

6. La Giunta Regionale d'Abruzzo si obbliga ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.

7. I nominativi ed i dati di contatto del Titolare e del Responsabile della protezione dati (RDP) sono pubblicati sul sito istituzionale della Regione Abruzzo, sezione Amministrazione trasparente, oltre che nella sezione "privacy" presente nella Home Page.

8. Ai fini di quanto previsto dal presente paragrafo la Giunta Regionale nomina con proprio atto il Responsabile della sicurezza dei sistemi informativi a cui vengono espressamente demandate le funzioni di cui al presente disciplinare e dei relativi allegati.

4. Registro informatizzato delle attività di trattamento

1. Il Titolare del trattamento, per il tramite dei DAT, provvede a redigere e mantenere aggiornato il Registro delle attività di trattamento di cui all'articolo 30, paragrafo 1 del GDPR, che reca almeno le seguenti informazioni:
    a) il nome ed i dati di contatto della Giunta Regionale d'Abruzzo, ivi compresi quelli relativi al DAT ed alla relativa Struttura, nonché quelli dell'eventuale co-titolare del trattamento e del RPD;
    b) le finalità del trattamento;
    c) la sintetica descrizione delle categorie di interessati, nonché delle 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 ed organizzative del trattamento adottate, secondo quanto indicato alla precedente sezione 3.

2. Il Registro è tenuto dal Titolare attraverso la struttura di cui al punto 10 della sezione 2.1. ed è costantemente aggiornato, per la parte di rispettiva competenza, dai DAT.

5. Registro delle categorie di attività relative al trattamento svolte per conto di un titolare

1. Nel caso in cui la Regione Abruzzo agisca in qualità di responsabile del trattamento per conto di altri distinti ed autonomi titolari, l'Ente è tenuto alla redazione del Registro dei trattamenti dei dati del Responsabile del trattamento, che deve recare le seguenti informazioni (art. 30, paragrafo 2 del GDPR):
    a) il nome ed 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, pseudominimizzazione, 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 ed organizzative del trattamento adottate, secondo quanto indicato alla precedente sezione 3.

2. Il registro è tenuto dal Responsabile del trattamento presso gli uffici della propria struttura organizzativa in forma telematica.

6. Valutazioni d'impatto sulla protezione dei dati (DPIA)

1. Nel caso in cui un tipo di trattamento, specie ove preveda in particolare l'uso di nuove tecnologie, presenti un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, per il tramite del DAT competente per materia, prima di effettuare il trattamento deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 GDPR, 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 meno 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 dei paragrafi 4, 5 e 6 dell'art. 35 GDPR.

3. La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. Fermo restando quanto indicato dal paragrafo 3 dell'art. 35, del GDPR, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:
   a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
   b) il trattamento, su larga scala, di categorie particolari di dati personali di cui al paragrafo 1 dell'articolo 9 GDPR, o di dati relativi a condanne penali e a reati di cui all'articolo 10 GDPR;
   c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

4. Ai fini di quanto previsto nella presente sezione si tiene conto dell'elenco delle tipologie di trattamenti soggetti al requisito di una DPIA ai sensi del paragrafo 1, dell'art. 35 GDPR, così come redatto e reso pubblico dall'Autorità di controllo.
5. Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati 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 soddisfi solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.

6. Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della DPIA ad un altro soggetto, interno o esterno all'Ente Regione.

7. 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.

8. Il Responsabile del trattamento deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria.

9. Il Responsabile della sicurezza dei sistemi informativi, ove nominato e/o l'ufficio competente per detti sistemi, forniscono supporto al Titolare per lo svolgimento della DPIA.

10. 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.

11. Il Responsabile della sicurezza dei sistemi informativi, ove 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.

12. 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 del paragrafo 1, dell'art. 35 GDPR;
    a) 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;
    b) se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del 25 maggio 2018 in condizioni specifiche che non hanno subito modifiche;
    c) 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.

13. 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 RPD 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 vengano modificate, sostituite od abrogate.

14. 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 (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 (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;
d) individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

15. 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.

16. 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 ed alla sanità pubblica.

17. 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.

18. È pubblicata sul sito istituzionale dell'Ente, in apposita sezione, una sintesi delle principali risultanze del processo di valutazione ovvero una semplice dichiarazione relativa all'effettuazione della DPIA.

7. Violazione dei dati personali (DATA BREACH)

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'Ente Regione Abruzzo.

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 deve avvenire entro 72 ore e comunque senza ingiustificato ritardo. Il DAT e/o il Responsabile del trattamento sono obbligati ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuti a conoscenza della violazione.

3. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità all'art. 25 GDPR (C75-C78), 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 pseudominimizzazione;
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 sia elevato, deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di far 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 categorie particolari di dati personali;
c) comprendere dati che possono accrescere ulteriormente i potenziali rischi;
d) comportare rischi imminenti e con un'elevata probabilità di accadimento;

e) impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni.

5. La notifica deve avere il contenuto minimo previsto dall'art. 33 GDPR, così come la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al medesimo art. 33.

6. Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate all'Autorità di controllo, nonché le circostanze ad 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 GDPR.

7. Il Titolare definisce le modalità operative adottate dalla Regione Abruzzo, per poter rispettare quanto previsto dagli articoli 33 e 34 del GDPR ed in particolare per definire il flusso di attività da attivarsi nel caso in cui dovesse manifestarsi un evento di violazione dei dati personali rispetto a quanto definito esplicitamente dalla normativa vigente nella procedura "Violazioni di Dati Personali (*Data Breach*)". A tal riguardo trova applicazione la "*Procedura per la Gestione delle Violazioni di Dati Personali (Data Breach)*" (Allegato C).

8. Esercizio diritti interessati

1. Il GDPR (articoli da 15 a 22) riconosce rilevanti diritti in materia di protezione dei dati personali, che possono essere esercitati rivolgendosi al Titolare del trattamento e che possono riguardare:
    a) accesso ai dati;
    b) rettifica dei dati;
    c) cancellazione dei dati (diritto all'oblio);
    d) limitazione del trattamento;
    e) portabilità dei dati;
    f) esercizio del diritto di opposizione;
    g) esercizio del diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato;
    h) proporre reclamo all'Autorità di controllo.

2. Il Titolare definisce le modalità e responsabilità per l'adozione di misure adeguate a fornire all'interessato tutte le informazioni da egli richieste secondo quanto previsto dalla normativa vigente in materia di privacy. A tal fine trova applicazione la "*Procedura "Diritti degli interessati*" (Allegato D).

3. Le richieste degli interessati possono pervenire unicamente tramite i canali previsti nell'informativa privacy pubblicata sul sito istituzionale[2].

9. Formazione dei soggetti del trattamento

1. La Regione Abruzzo, ai fini di garantire la migliore tutela dei dati personali, assicura l'attivazione e la realizzazione di percorsi formativi che tengano conto anche della funzione ricoperta dai destinatari all'interno dell'organizzazione regionale.

2. Al fine di garantire a tutto il personale una conoscenza di base in tema di protezione dei dati, nonché di consolidare e rafforzare le competenze specialistiche delle risorse umane direttamente coinvolte nelle attività connesse alla protezione dei dati, è pianificata la realizzazione di specifici percorsi formativi rivolti ai seguenti destinatari:
DAT; SAT; Personale dell'Ufficio di Supporto del RPD; Personale della struttura di supporto del Titolare; Responsabile per la sicurezza dei sistemi informativi.

3. Nell'ambito dei percorsi formativi devono essere progressivamente introdotti strumenti di verifica dell'apprendimento.

4. La definizione dei corsi di formazione e dei relativi contenuti per le diverse figure e ruoli devono essere differenziati in funzione della tipologia di destinatario e degli obiettivi formativi definiti.

5. Nell'ambito dell'ordinario percorso formativo per il personale dipendente di nuova assunzione deve essere previsto un modulo specifico di formazione base sulla normativa relativa alla protezione dei dati personali.

6. L'aggiornamento periodico delle conoscenze sarà garantito attraverso l'attivazione di corsi anche in modalità e-learning.

7. Ai fini di quanto previsto dalla presente sezione viene definito un apposito Piano di formazione sulla privacy da parte di uno specifico gruppo di lavoro composto dal Responsabile della Gestione Documentale (RGP), dal Responsabile per la sicurezza dei sistemi informativi, dal Dirigente del Servizio competente in materia di formazione del personale della Giunta Regionale e dal RPD.

[2] Allegato E) "Informativa generale".

10. Norme di prima attuazione

1. In fase di prima applicazione ed al fine di accelerare il processo di adeguamento al GDPR, dalla data di adozione del presente Disciplinare da parte della Giunta Regionale, i DAT sono autorizzati al trattamento dei dati personali nel rispetto di quanto previsto dalla "*Procedura per la designazione dei Soggetti autorizzati al trattamento dei dati personali e relativa attribuzione di responsabilità*" (Allegato A).
2. I DAT, entro trenta (30) giorni dalla comunicazione del provvedimento di approvazione del presente Disciplinare da parte della Giunta Regionale provvedono, nell'ambito delle strutture di rispettiva competenza, alla designazione dei Soggetti Autorizzati al Trattamento dei dati personali (SAT) secondo la "*Procedura per la designazione dei Soggetti autorizzati al trattamento dei dati personali e relativa attribuzione di responsabilità*" (Allegato A).

11. Rinvio

1. Per tutto quanto non espressamente disciplinato nelle precedenti sezioni del presente Disciplinare e nei relativi allegati si applicano le disposizioni del GDPR e del Codice della Protezione dei Dati Personali, così come modificato dal D.Lgs. 101/2018.

12. Allegati

1. I seguenti allegati formano parte integrante e sostanziale del presente disciplinare:

   - Allegato A - "Procedura per la designazione dei Soggetti autorizzati al trattamento dei dati personali e relativa attribuzione di responsabilità";
   - Allegato B - "Procedura per la gestione degli accordi di designazione del Responsabile del Trattamento";
   - Allegato C - "Procedura per la Gestione delle Violazioni di Dati Personali (Data Breach)";
   - Allegato D - "Procedura "Diritti degli interessati".
   - Allegato E – "Informativa generale".

Per eventuali approfondimenti sui contenuti del presente Disciplinare si fa rinvio ai seguenti link: https://www.garanteprivacy.it/regolamentoue e https://protezionedatipersonali.it/

APPENDICE NORMATIVA

Riferimenti alle sezioni del Disciplinare	**Norme del Regolamento (UE) 679/2016**
Sezione 2.1 (Titolare del trattamento)	**Articolo 5** Principi *applicabili al trattamento di dati personali* 1. I dati 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, conformemente all'articolo 89, paragrafo 1, 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 («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 («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, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»); f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

	2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).
Sezione 2.4 (Responsabile del trattamento dati (RT)) **Sezione 6** (Valutazioni d'impatto sulla protezione dei dati)	**Articolo 9** *Trattamento di categorie particolari di dati personali* 1. E' vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. 2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi: a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1; b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato; c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso; d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato; e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato; f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;

	g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato; h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3; i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale; j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato. 3. I dati personali di cui al paragrafo 1 possono essere trattati per le finalità di cui al paragrafo 2, lettera h), se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti. 4. Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute.
Sezione 2.1 (Titolare del trattamento)	**Articolo 13** *Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato*

	1. In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni: a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante; b) i dati di contatto del responsabile della protezione dei dati, ove applicabile; c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento; d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi; e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali; f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, paragrafo 1, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili. (6) 2. In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente: a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati; (6) c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca; d) il diritto di proporre reclamo a un'autorità di controllo; e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati

	personali nonché le possibili conseguenze della mancata comunicazione di tali dati; f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato. 3. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al paragrafo 2. 4. I paragrafi 1, 2 e 3 non si applicano se e nella misura in cui l'interessato dispone già delle informazioni.
Sezione 2.1 (Titolare del trattamento)	**Articolo 14** *Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato* 1. Qualora i dati non siano stati ottenuti presso l'interessato, il titolare del trattamento fornisce all'interessato le seguenti informazioni: a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante; b) i dati di contatto del responsabile della protezione dei dati, ove applicabile; c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento; d) le categorie di dati personali in questione; e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali; f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un destinatario in un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, paragrafo 1, secondo comma, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili. (7) 2. Oltre alle informazioni di cui al paragrafo 1, il titolare del trattamento fornisce all'interessato le seguenti informazioni necessarie per garantire un trattamento corretto e trasparente nei confronti dell'interessato:

	a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; b) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi; c) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati; d) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca; e) il diritto di proporre reclamo a un'autorità di controllo; f) la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico; g) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato. 3. Il titolare del trattamento fornisce le informazioni di cui ai paragrafi 1 e 2: a) entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati; b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato; oppure c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali. 4. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati ottenuti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni informazione pertinente di cui al paragrafo 2. 5. I paragrafi da 1 a 4 non si applicano se e nella misura in cui: a) l'interessato dispone già delle informazioni; b) comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di

	ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e le garanzie di cui all'articolo 89, paragrafo 1, o nella misura in cui l'obbligo di cui al paragrafo 1 del presente articolo rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni; c) l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato; oppure d) qualora i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri, compreso un obbligo di segretezza previsto per legge.
Sezione 2.1 (Titolare del trattamento) **Sezione 8** (Esercizio diritti interessati)	**Articolo 15** *Diritto di accesso dell'interessato* 1. 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, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

	2. Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento. 3. 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. 4. Il diritto di ottenere una copia di cui al paragrafo 3 non deve ledere i diritti e le libertà altrui.
Sezione 2.1 (Titolare del trattamento) **Sezione 8** (Esercizio diritti interessati)	**Articolo 16** *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.
Sezione 2.1 (Titolare del trattamento) **Sezione 8** (Esercizio diritti interessati)	**Articolo 17** *Diritto alla cancellazione («diritto all'oblio»)* 1. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti: a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento; c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2; d) i dati personali sono stati trattati illecitamente; e) i dati personali devono essere cancellati per adempiere un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; [(8)]

	f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1. 2. Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali. 3. I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario: a) per l'esercizio del diritto alla libertà di espressione e di informazione; b) per l'adempimento di un obbligo giuridico 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; (8) c) 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; d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
Sezione 2.1 (Titolare del trattamento) **Sezione 8** (Esercizio diritti interessati)	**Articolo 18** *Diritto di limitazione di trattamento* 1. L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi: a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali; b) il trattamento 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, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato. 2. Se il trattamento è limitato a norma del paragrafo 1, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro. 3. L'interessato che ha ottenuto la limitazione del trattamento a norma del paragrafo 1 è informato dal titolare del trattamento prima che detta limitazione sia revocata.
Sezione 2.1 (Titolare del trattamento) **Sezione 8** (Esercizio diritti interessati)	**Articolo 19** *Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento* Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma dell'articolo 16, dell'articolo 17, paragrafo 1, e dell'articolo 18, 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.
Sezione 2.1 (Titolare del trattamento) **Sezione 8** (Esercizio diritti interessati)	**Articolo 20** *Diritto alla portabilità dei dati* 1. L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora: a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e b) il trattamento sia effettuato con mezzi automatizzati. 2. Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile. 3. L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 17. Tale diritto non si applica al

	trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. 4. Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui.
Sezione 2.1 (Titolare del trattamento) **Sezione 8** (Esercizio diritti interessati)	**Articolo 21** *Diritto di opposizione* 1. 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), 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. 2. Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto. 3. Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità. 4. Il diritto di cui ai paragrafi 1 e 2 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. 5. 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. 6. Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguardano, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico. (9)
Sezione 2.1 (Titolare del trattamento)	**Articolo 22** *Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione* 1. L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato,

Sezione 8 (Esercizio diritti interessati)	compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona. 2. Il paragrafo 1 non si applica nel caso in cui la decisione: a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; c) si basi sul consenso esplicito dell'interessato. 3. Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione. 4. Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.
Sezione 2.4 (Responsabili del trattamento dati (RT))	**Articolo 28** *Responsabile del trattamento* 1. Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato. 2. Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche. 3. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie

	di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento: a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico; b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza; c) adotti tutte le misure richieste ai sensi dell'articolo 32; d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento; e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui 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 di cui al capo III; f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento; g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato. Con riguardo alla lettera h) del primo comma, il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

	4. Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile. 5. L'adesione da parte del responsabile del trattamento a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui ai paragrafi 1 e 4 del presente articolo. 6. Fatto salvo un contratto individuale tra il titolare del trattamento e il responsabile del trattamento, il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 del presente articolo può basarsi, in tutto o in parte, su clausole contrattuali tipo di cui ai paragrafi 7 e 8 del presente articolo, anche laddove siano parte di una certificazione concessa al titolare del trattamento o al responsabile del trattamento ai sensi degli articoli 42 e 43. 7. La Commissione può stabilire clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo e secondo la procedura d'esame di cui all'articolo 93, paragrafo 2. 8. Un'autorità di controllo può adottare clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo in conformità del meccanismo di coerenza di cui all'articolo 63. 9. Il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 è stipulato in forma scritta, anche in formato elettronico. 10. Fatti salvi gli articoli 82, 83 e 84, se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione.
Sezione 4 (Registro delle attività di trattamento)	**Articolo 30** *Registri delle attività di trattamento* 1. Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento

Sezione 5 (Registro delle categorie di attività relative al trattamento svolte per conto di un titolare)	svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni: a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati; b) le finalità del trattamento; c) una descrizione delle categorie di interessati e delle categorie di dati personali; d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali; e) 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; f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati; g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1. 2. Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un 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. 3. I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.

	4. Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo. 5. Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.
Sezione 2.2 Delegato al Trattamento dei dati (DAT) **Sezione 2.3** Soggetto Autorizzato al trattamento dei dati (SAT)	**Articolo 32** *Sicurezza del trattamento* 1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, 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, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. 2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. 3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo. 4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal

	titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.
Sezione 2.2 (Delegato al Trattamento dei dati (DAT))	**Articolo 33** *Notifica di una violazione dei dati personali all'autorità di controllo* 1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo. 2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione. 3. La notifica di cui al paragrafo 1 deve almeno: a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione; b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni; c) descrivere le probabili conseguenze della violazione dei dati personali; d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi. 4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo. 5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.
Sezione 2.2 (Delegato al Trattamento dei dati (DAT))	**Articolo 34** *Comunicazione di una violazione dei dati personali all'interessato* 1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone

Sezione 7 (Violazione dei dati personali)	fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo. 2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d). 3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni: a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura; b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1; c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia. 4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.
Sezione 2.1 (Titolare del trattamento) **Sezione 2.2** (Delegato al Trattamento dei dati (DAT)) **Sezione 6** (Valutazioni d'impatto sulla protezione dei dati) **Sezione 7** (Violazione dei dati personali)	**Articolo 35** *Valutazione d'impatto sulla protezione dei dati* 1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi. 2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.

	3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti: a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche; b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico. 4. L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68. 5. L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato. 6. Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione. 7. La valutazione contiene almeno: a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento; b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione. 8. Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte

	di questi ultimi dei codici di condotta approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati. 9. Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti. 10. Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento. 11. Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.
Sezione 2.2 (Delegato al Trattamento dei dati (DAT)) **Sezione 2.5** (Responsabile della protezione dati (RPD/DPO))	**Articolo 36** *Consultazione preventiva* 1. Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio. 2. Se ritiene che il trattamento previsto di cui al paragrafo 1 violi il presente regolamento, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, l'autorità di controllo fornisce, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un parere scritto al titolare del trattamento e, ove applicabile, al responsabile del trattamento e può avvalersi dei poteri di cui all'articolo 58. Tale periodo può essere prorogato di sei settimane, tenendo conto della complessità del trattamento previsto. L'autorità di controllo informa il titolare del trattamento e, ove applicabile, il responsabile del trattamento di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione. La decorrenza dei termini può

	essere sospesa fino all'ottenimento da parte dell'autorità di controllo delle informazioni richieste ai fini della consultazione. 3. Al momento di consultare l'autorità di controllo ai sensi del paragrafo 1, il titolare del trattamento comunica all'autorità di controllo: a) ove applicabile, le rispettive responsabilità del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo imprenditoriale; b) le finalità e i mezzi del trattamento previsto; c) le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del presente regolamento; d) ove applicabile, i dati di contatto del responsabile della protezione dei dati; (11) e) la valutazione d'impatto sulla protezione dei dati di cui all'articolo 35; e (11) f) ogni altra informazione richiesta dall'autorità di controllo. 4. Gli Stati membri consultano l'autorità di controllo durante l'elaborazione di una proposta di atto legislativo che deve essere adottato dai parlamenti nazionali o di misura regolamentare basata su detto atto legislativo relativamente al trattamento. 5. Nonostante il paragrafo 1, il diritto degli Stati membri può prescrivere che i titolari del trattamento consultino l'autorità di controllo, e ne ottengano l'autorizzazione preliminare, in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica.
Sezione 2 (Organigramma privacy)	**Articolo 37** *Designazione del responsabile della protezione dei dati* 1. Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta: a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali; b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga

	scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10. 2. Un gruppo imprenditoriale può nominare un unico responsabile della protezione dei dati, a condizione che un responsabile della protezione dei dati sia facilmente raggiungibile da ciascuno stabilimento. 3. Qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione. 4. Nei casi diversi da quelli di cui al paragrafo 1, il titolare del trattamento, il responsabile del trattamento o le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o di responsabili del trattamento possono o, se previsto dal diritto dell'Unione o degli Stati membri, devono designare un responsabile della protezione dei dati. Il responsabile della protezione dei dati può agire per dette associazioni e altri organismi rappresentanti i titolari del trattamento o i responsabili del trattamento. 5. Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39. 6. Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi. 7. Il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo.
	Articolo 39 *Compiti del responsabile della protezione dei dati* 1. Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti: a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati; b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla

	protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo; c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35; d) cooperare con l'autorità di controllo; e e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione. 2. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.